

BEVEILIGING EN CONTINUÏTEIT VAN BEDRIJFSPROCESSEN

DE VISIE VAN GETRONICS



2008 © **Getronics** | Alle rechten voorbehouden. Niets uit deze uitgave mag openbaar worden gemaakt of verveelvoudigd, opgeslagen in een dataverwerkend systeem of uitgezonden in enige vorm door middel van druk, fotokopie of welke andere wijze dan ook zonder voorafgaande schriftelijke toestemming van de directie van Getronics Nederland BV.

INHOUDSOPGAVE

| | | |
|-------|--|----|
| 1 | WAAROM DIT BOEKJE | 05 |
| 1.1 | PERSPECTIEF | 06 |
| 1.1.1 | OUT OF BUSINESS? | 06 |
| 1.1.2 | ONTWIKKELING VAN INFORMATIEBEVEILIGING | 08 |
| 1.2 | CONSTANTE FACTOREN IN EEN VERANDERENDE OMGEVING | 10 |
| 1.2.1 | DE CONSTANTE FACTOREN | 10 |
| 1.2.2 | DE VERANDERENDE OMGEVING | 13 |
| 1.2.3 | HERORIËNTATIE | 13 |
| 1.2.4 | INHERENTE KWALITEIT | 14 |
| 1.2.5 | WAT BEDREIGT ONS? | 17 |
| 1.2.6 | LEVENSTIJL EN KOSTEN | 18 |
| 1.3 | VANZELFSPREKEND | 19 |
| 1.3.1 | PLEZIER? | 19 |
| 1.3.2 | IN CONTROL | 19 |
| 2 | DE TOREN | 21 |
| 2.1 | HET MODEL | 22 |
| 2.2 | VALLEN | 23 |
| 2.3 | SCHUDDEN EN KANTELEN | 24 |
| 3 | KLANTEN EN LEVERANCIERS | 27 |
| 3.1 | DIFFUSE GRENZEN | 27 |
| 3.2 | DIT WAS (NIET) DE AFSPRAAK | 28 |
| 3.3 | DE MENS, DE NORM EN DE WAARDE | 28 |
| 3.3.1 | VERHARDING | 29 |
| 3.3.2 | JOBHOPPING | 29 |
| 3.3.3 | MORELE AFSTAND | 30 |
| 3.4 | VERTROUWEN EN CONTROLE | 30 |

| | | |
|--------|------------------------------------|----|
| 4 | MAATREGELEN IN DE JUISTE PROPORТИE | 33 |
| 4.1 | KOSTEN EN BATEN | 34 |
| 4.2 | DE STRUCTUUR | 35 |
| 4.3 | ZWAKKE SCHAKELS | 37 |
| 5 | MENSEN EN MIDDELEN | 39 |
| 5.1.1 | PERSONEELSWISSELING | 39 |
| 5.1.2 | OPLEIDING EN BEWUSTWORDING | 40 |
| 5.1.3 | MENSELIJK FALEN | 41 |
| 5.1.4 | MISBRUIK | 41 |
| 5.1.5 | CLASSIFICATIE VAN MIDDELEN | 43 |
| 5.1.6 | INTERNET IS EVERYWHERE | 43 |
| 5.1.7 | FALENDE SYSTEMEN | 44 |
| 5.1.8 | ONTWIKKELFOUTEN | 45 |
| 5.1.9 | ALTIJD BESCHIKBAAR | 47 |
| 5.1.10 | MANAGEMENTCYCLUS | 47 |
| 6 | IN HOEVERRE 'IN CONTROL' | 49 |
| 6.1 | WAT DE WET DOET | 50 |
| 6.2 | RISICO MANAGEMENT | 51 |
| 6.3 | WANNEER BEN IK ECHT 'IN CONTROL'? | 53 |
| 7 | CONCLUSIE EN VISIE | 55 |
| 7.1 | ONZICHTBAAR EN AGRESSIEVER | 55 |
| 7.2 | INTEGRALE AANDACHT EN ARCHITECTUUR | 56 |
| 7.3 | VISIE | 57 |
| 7.4 | UITBESTEDEN? | 58 |
| 7.5 | COMPLEXE VRIJHEID | 59 |
| 7.6 | CONCLUSIE | 60 |

‘BUSINESS CONTINUITY MANAGEMENT:
WEER ZO’N HYPE! NATUURLIJK IS HET
BELANGRIJK, MAAR KIJK EENS WAT ER
NOG MEER OP M’N BORDJE LIGT..’

‘SECURITY MANAGERS HOREN WAT MIJ
BETREFT IN DEZELFDE CATEGORIE ALS
BELASTINGAMBTENAREN EN ACCOUNTANTS:
IK WEET WEL DAT ZE NODIG ZIJN,
MAAR IK ZIE ZE LIEVER GAAN DAN KOMEN.’

‘IK HEB BINNEN MIJN UNIT DE AFSPRAAK
GEMAAKT DAT WIJ ALLEMAAL ELKAARS WACHT-
WOORD MOETEN KENNEN, DAT IS MAKKELIJK
ALS IEMAND EEN KEER AFWEZIG IS..’

Herkent u dit? Wel eens van gehoord? Of denkt u er zelf stiekem ook zo over? Wellicht bent u verbaasd dat er (weer) een uitgave over continuïteit en beveiliging is volgeschreven. Of bent u blij dat er weer eens serieuze aandacht aan wordt besteed?

1

WAAROM DIT BOEKJE?

Nieuw belang

Er is (hernieuwde) belangstelling voor het zeker stellen van de bedrijfscontinuïteit. Business Continuity Management, Corporate Governance, Compliance, Security en Risk Management zijn begrippen waar al vele congressen aan zijn gewijd. Het zijn aan elkaar gerelateerde en in elkaar overlopende disciplines.

Recente wet- en regelgeving hebben verstrekkende gevolgen waardoor directies en managers tot maatregelen zijn gedwongen die bewijzen dat zij 'in control' zijn. De continuïteit van een onderneming moet aantoonbaar gewaarborgd worden. Er moet zelfs publiekelijk verantwoording worden afgelegd.

Dit boekje is geen theoretische verhandeling over verschillende benaderingen van bedrijfscontinuïteit en databeveiliging. Ook niet over hoe problemen hiermee moeten worden opgelost. Het is evenmin een technisch verhaal. Maar het is wél een beschouwing over de algemene trend dat we zekerheden willen scheppen in een weerbarstige omgeving. Daarbij staat de continuïteit van de bedrijfsprocessen centraal. Een onderneming die afhankelijk is van informatietechnologie, moet zich wapenen tegen omstandigheden die de continuïteit kunnen aantasten. Aantasting die – in welke vorm dan ook – inbreuk doet op de voortgang van de bedrijfsprocessen.

WE SCHETSEN IN DIT BOEKJE DE VERBANDEN EN DE MANIER
WAAROP GETRONICS TEGEN DE MATERIE AANKIJKT.

1.1 PERSPECTIEF

1.1.1 Out of business?

De razendsnelle ontwikkelingen in de technologie beïnvloeden alle facetten van de maatschappij. Voor ondernemers brengt dat kansen met zich mee, maar ook bedreigingen. Het zijn ontwikkelingen die systematisch onderzoek vergen naar maatregelen die onze bedrijven optimaal laten functioneren en discontinuïteit van bedrijfsprocessen voorkomen. Bovendien moeten we die maatregelen in stand houden en controleren.

We spiegelen ons voortdurend aan de veranderende omgeving. Blevten toepassingen tot voor kort beperkt tot binnen de muren van bedrijven of bedrijfsfuncties, tegenwoordig willen we onze klanten rechtstreeks toegang geven tot de backoffice en werken we samen met ketenpartners die we tot ver in onze productieprocessen willen laten meedoen.

Want waarom zou een klant 'zijn dossier' niet vanaf huis mogen inzien en muteren? Waarom zou de burger naar een loket moeten om van de overheid iets gedaan te krijgen? Of naar een bankgebouw als hij thuis zijn bankzaken kan afhandelen? Waarom zouden handmatige werkzaamheden een order-, inkoop-, fabricage-, opslag- en verzendproces stagneren? Waarom moeten onze beheerders ter plaatse zijn als ze thuis allerlei processen kunnen beheren? Dat kan vanaf huis, of beter nog, onderweg. We werken 'anywhere at any time on any device'. We werken als bedrijf in een keten van met elkaar samenwerkende bedrijven. Waarom zouden we onze ICT niet op elkaar aansluiten?

Informatietechnologie schept ongekende mogelijkheden, maar door de toenemende afhankelijkheid van deze technologie is de maatschappelijke kwetsbaarheid en de risico's die dat met zich meebrengt een

bron van zorg. De bescherming van informatietechnologie is dus van groot belang.

Heb ik de zekerheid?

We hebben te maken met vragen als: hoe weet ik zeker dat de gebruiker degene is die hij of zij zegt te zijn? Kloppen de gegevens nog wel en wordt er tijdens het gegevenstransport niet iets verminkt, of erger nog: bewust gemanipuleerd? Heb ik de zekerheid dat het geheel 24 uur per dag goed functioneert? En als het stagneert, kan ik de gevolgen dan opvangen?

De kans op ongelukken met een hoge impact wordt hoger en de schade groter. Het wordt steeds complexer om schade volledig te herstellen. Bedrijven die niet snel herstellen na een calamiteit zijn 'out of business'. Klanten zijn dan allang naar de concurrent overgestapt. Dat kost die klant al moeite (en geld) genoeg. Waarom zouden ze dat proces nog eens doormaken

om weer terug te keren? Die klant is dus geen klant meer.

Behalve een ongeluk kan ook gericht terrorisme via informatietechnologie maatschappelijke ontwrichting veroorzaken. Het actieplan 'Terrorismebestrijding en veiligheid' van de Nederlandse overheid vraagt niet voor niets expliciete aandacht voor het bestrijden van computer-criminaliteit.

Kortom, willen we 'in business' blijven, dan zullen we onze geautomatiseerde bedrijfsprocessen moeten beschermen. De niet meer weg te denken en alomtegenwoordige informatietechnologie – en daarmee de kwetsbaarheid van onze bedrijfsvoering – dwingt ons voortdurend om die kwetsbaarheid tot een aanvaardbaar niveau terug te brengen.

BEDRIJVEN DIE NIET SNEL HERSTELLEN
NA EEN CALAMITEIT ZIJN 'OUT OF BUSINESS'.
KLANTEN ZIJN DAN ALLANG
NAAR DE CONCURRENT OVERGESTAPT.

De bedrijven en organisaties die zich deze vragen hebben gesteld en beantwoord, die dit voor elkaar hebben, lopen voor op hun concurrenten. Hun zakelijke risico's zijn kleiner en ze hoeven minder hoge risicoreserveringen aan te houden. Deze bedrijven doen dus al, in enigerlei vorm, aan Business Continuity Management.

1.1.2 De geschiedenis van de informatiebeveiliging

Is er eigenlijk iets nieuws onder de zon? Hebben we te maken met een principieel andere kijk op Business Continuity Management, informatiebeveiliging, ICT-security, gegevensbescherming of hoe we het ook maar willen noemen? Laten we kijken hoe het vakgebied informatiebeveiliging zich ontwikkelde. Begin jaren zeventig van de vorige eeuw waren we trots op onze computers: bij commerciële bedrijven en rekencentra stonden ze letterlijk in de etalage.

Iedereen moest kunnen zien hoe modern zo'n bedrijf wel niet was. Verbindingen met de buitenwereld in de vorm van netwerken bestonden niet. Een stevig gebouw was voldoende om onheil van buiten te weren. Maar de activiteiten van de Brigade Rosso (Italië), de Rote Armee Fraktion (Duitsland) en de Communistische Strijdende Cellen (België), die rekencentra van bijvoorbeeld de overheid stillegden, maakten duidelijk dat informatietechnologie een cruciale factor in het maatschappelijk

functioneren begon te worden.

De etalages verdwenen en het systematisch nadenken over de beveiliging van rekencentra begon. Naarmate de tijd verstreek, kwamen er meer en meer aanleidingen om over informatiebeveiliging na te denken. Soms leidde dat tot aangepaste wetgeving. Enkele voorbeelden:

- Het verzet tegen het geautomatiseerd verwerken van gegevens uit de volkstelling leidde tot privacywetgeving.
- Activiteiten van hackers moesten de aanzet zijn voor mogelijkheden tot strafvervolging: de wetgeving met betrekking tot computercriminaliteit ontstond.
- De wens om in de digitale wereld te kunnen beschikken over wettige handtekeningen noopte tot wetgeving over de elektronische handtekening.
- Grote fraudezaken waren aanleiding voor overheden om te komen met wet- en regelgeving waarin bestuurders aangepakt kunnen worden bij niet-integer handelen (Sarbanes Oxley en Code Tabaksblatt).
- Onder druk van de 24-uurs-economie moesten informatietechnologie-infrastructuren 24 uur per dag en 365 dagen per jaar functioneren en betrouwbaar zijn. Een andere kijk op transactie- en batchverwerking ontstond. Nieuwe concepten voor uitwijk na een ramp moesten worden bedacht. Want wie kan

nog drie dagen wachten voordat de IT-infrastructuur weer in de lucht is?

- Omdat een groot deel van het economisch handelen zich via computers ging afspelen, werd dit ook het terrein van fraudeurs en criminaliteit. Inbreken in computers, manipuleren van gegevens: we moesten er rekening mee gaan houden.
- Lokale economieën globaliseren en de onderlinge afhankelijkheden daarin nemen toe. Outsourcingpraktijken maken ons afhankelijk van partijen en hun onderaannemers waarvan we niet eens meer weten waar ze zich op de wereld bevinden.

Geen paniekbeleid, steeds meer regels

We kwamen tot de ontdekking dat het ad hoc reageren op incidenten moest worden vervangen door een permanente vorm van risicomanagement die in onze bedrijfsprocessen is ingebakken. Los van formele wet- en regelgeving kwamen bedrijven en brancheverenigingen ook tot de conclusie dat het beschermen van informatie en bedrijfsprocessen serieuze taken waren geworden.

Accountants oordeelden dat zij eigenlijk geen verklaringen over jaarrekeningen konden geven als die jaarrekeningen – inclusief bedrijfsprocessen – via de computer tot stand waren gekomen. Dan zou er toch ook een oordeel moeten worden gegeven over de werking van de

processen in die computer? Daarmee ontstond een nieuw specialisme: dat van de EDP-auditor (tegenwoordig IT-auditor). Ook deze specialisten verenigden zich en begonnen eigen richtlijnen en gedragscodes op te stellen. En de accountants kwamen met uitgebreide voorstellen voor normering en uniformering.

De Nederlandsche Bank stelde verplicht dat in de verklaringen van accountants in de jaarrekeningen van banken ook uitspraken moesten komen over de beveiliging van de ICT. Het Basel II akkoord voor banken had als belangrijk doel de risico's in de ketenafhankelijkheid van banken te verkleinen. Een aantal grote internationale bedrijven verenigde zich rond het onderwerp informatiebeveiliging. Daaruit ontstond in Engeland een standaardaanpak voor Informatiebeveiliging (BS 7799), die in Nederland werd vertaald door het ministerie van Economische Zaken en overgenomen als de Code voor Informatie Beveiliging (CvIB). Inmiddels is deze standaard door de ISO geadopteerd als ISO27001 en daarmee een wereldstandaard geworden.

De Nederlandse overheid gaf 'Voorschrift Informatiebeveiliging Rijksdienst 94' (VIR) uit over hoe overheidsinstellingen moeten omgaan met het inrichten en in stand houden van een adequaat niveau van beveiliging. Het VIR kreeg in 2007 een herziene editie en er ontstond een VIR voor Bijzondere Informatie (VIR-BI).

SAS70-verklaringen en Third Party Mededelingen (TPM) werden gebaseerd op ervaringen van auditors over de zekerheid waarmee bedrijven op hun informatietechnologie kunnen steunen waardoor ze bij hun klanten een bepaalde mate van vertrouwen wekken. Op het gebied van Business Continuity Management ontstond de norm BS25999.

Ook hier zien we de verschuiving van ad-hocmaatregelen op grond van incidenten en veranderende omstandigheden naar een gestandaardiseerde en gesystematiseerde aanpak, ingebed in een managementcyclus.

1.2 CONSTATE FACTOREN IN EEN VERANDERENDE OMGEVING

1.2.1 Overeenstemming

In de loop van de tijd zijn modellen en begrippen ontstaan waarover in het vakgebied informatiebeveiliging consensus heerst. Natuurlijk zijn er varianten, maar in de basis is een aantal begrippen onveranderd en nog steeds actueel.

ALS HET GAAT OM DE BESCHERMING VAN GEGEVENS, GEGEVENSVERWERKING EN -TRANSPORT GELDEN NOG STEEDS DRIE WAARDEN:

- Vertrouwelijkheid (bedrijfs- en/of persoonsvertrouwelijkheid);
- Integriteit (juistheid en volledigheid);
- Beschikbaarheid (beschikbaar wanneer nodig).

Daarnaast is er tegenwoordig veel aandacht voor de zogenaamde 'accountability' en 'audit trail'; het kunnen bewijzen wie wanneer welke informatie heeft gemuteerd, specifiek op financiële en logistieke applicaties.

Inbreuk – door wat voor oorzaak dan ook – op één of meerdere van deze waarden heeft ongewenste effecten op bedrijfsprocessen en moet bestreden worden door een evenwichtig geheel van maatregelen. Maatregelen zijn er in allerlei soorten, variërend in diepgang. In het boekje 'Gegevensbescherming'¹ staat een praktisch model voor het opzetten en invoeren van een systeem van gegevensbeschermende maatregelen wordt een model geïntroduceerd dat de hierboven genoemde waarden in relatie brengt met de te nemen maatregelen. Het model dat dit boekje beschrijft is nog steeds actueel en wordt in de praktijk nog steeds toegepast.

DE SOORTEN MAATREGELEN DIE WORDEN BESCHREVEN, ZIJN:

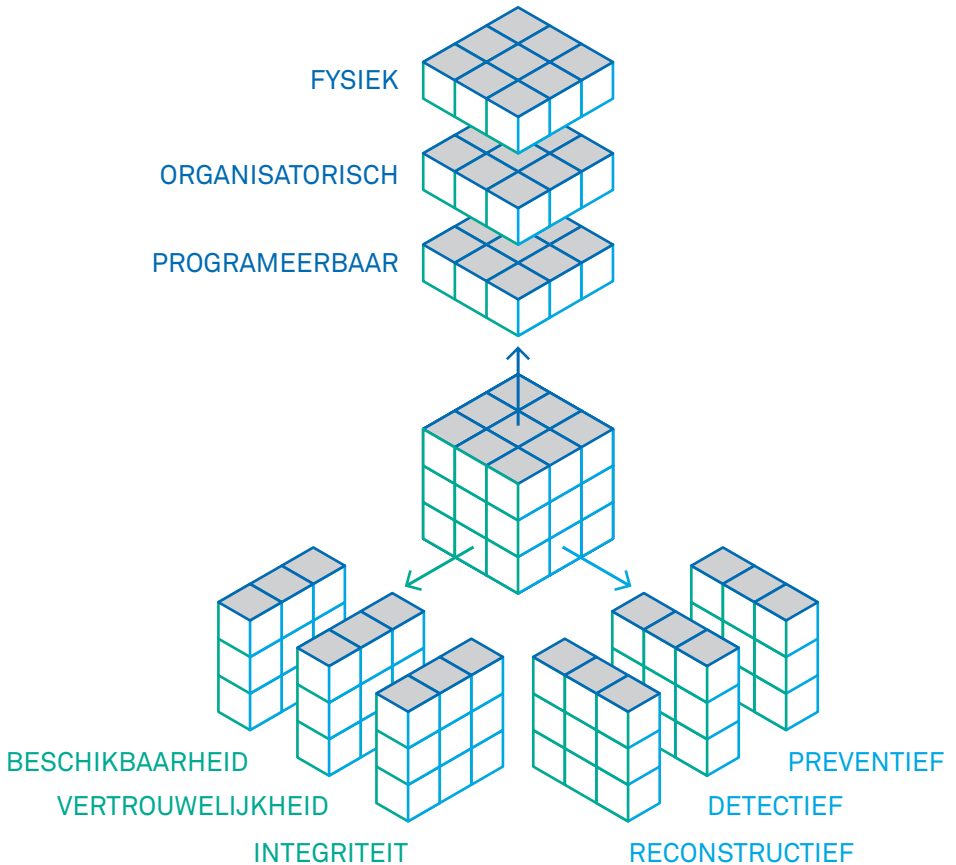
- Fysieke: brandwerende constructies, veiligheidszones, chipkaarten;
- Organisatorische: beschreven instructies en administratieve organisatie, veiligheidsonderzoeken, gedragscodes;
- Programmeerbare: username/wachtwoord, cryptografie, identity-management, digitale handtekening.

MAATREGELEN ZIJN VERDER NOG TE KARAKTERISEREN NAAR HUN AARD:

- Preventief: voorkomen dat inbreuken optreden;
- Detectief: tijdig signaleren van inbreuken en beperken van schade;
- Reconstructief: herstellen van de gewenste toestand na een inbreuk.

1. Gegevensbescherming. Een praktisch model voor het opzetten en invoeren van een systeem van gegevensbeschermende maatregelen. J.F. Bautz, A. Brouwer, A.J.F.M. Jongenelen. Kluwer, 1987, ISBN 902671130.

DE RELATIE TUSSEN DE TE BESCHERMEN WAARDEN EN DE SOORTEN
 MAATREGELEN NAAR HUN AARD LATEN ZICH SAMENVATTEN EN
 PRESENTEREN IN DE VOLGENDE KUBUS:



Figuur 1 Samenhang en typen maatregelen

2. Visie op Informatiebeveiliging, RCC, ISBN 90-803102-3-9
3. Informatiebeveiliging in de praktijk, RCC, ISBN 90-803102-2-0

Het toenmalige RCC (een van de rechtsvoorgangers van Getronics) heeft in de eigen publicaties 'Visie op Informatiebeveiliging'² en 'Informatiebeveiliging in de praktijk'³ deze kubus gestalte gegeven door aan elk van de 27 minikubusjes een waarde toe te schrijven die moet worden beschermd, naast de soort en aard van de maatregelen die dat moeten bewerkstelligen.

1.2.2 De veranderende omgeving

Het is een illusie om te veronderstellen dat met het eenmalig goed inrichten van een IT-beveiliging de kous af is. De informatie-technologie, de toepassingen, het gebruik ervan, en de inbreuken, aanvallen en dreigingen veranderen. Wie had bijvoorbeeld tien jaar geleden de impact – juist ook op de beveiliging – kunnen vermoeden die het internet met zich mee zou brengen?

Als gevolg van deze veranderingen zijn ook eerder genomen beveiligingsmaatregelen aan een voortdurende evaluatie onderhevig. Risicomanagement is in dit verband dan ook een kernbegrip: op basis van een gebruikelijke managementcyclus (beleid maken, analyseren, uitvoeren, controleren en bijstellen) moet er voortdurend en systematisch gezocht worden naar het evenwicht tussen de veranderende omgeving en de technologie, de eventuele inbreuken, en de te nemen maatregelen met het beschikbare budget. We zien intussen een ontwikkeling die zich richt op geïntegreerde of integrale

beveiliging. Daarbij wordt IT-beveiliging, fysieke beveiliging, maar ook persoonsbeveiliging in samenhang bekeken en hier en daar zelfs al door geïntegreerde technieken ondersteund.

1.2.3 Heroriëntatie

Er is een omslag gaande van reactief investeren in beveiliging op ad-hocbasis naar een meer proactieve en gesystematiseerde benadering. Standaardoplossingen krijgen de voorkeur boven maatwerk. Er is behoefte aan Key Performance Indicatoren (KPI's) waarmee de prestaties van securitymaatregelen continu worden gemeten. Een standaard als de ISO27001 verlangt expliciete benoeming van de KPI's, zodat ondermaatse beveiligingsprocessen en maatregelen tijdig kunnen worden aangepakt.

Outsourcen erg?

Waar voorheen nog wel huiver bestond om beveiliging te outsourcen, wordt dit steeds meer gebruikelijk. In navolging van het uitbesteden van fysieke beveiliging wordt het outtassen en outsourcen van securityfuncties gewoon. Gebrek aan kennis, hoge kosten en politieke tegenstellingen hielden gewenste securityontwikkelingen nogal eens tegen. Door deze over te dragen aan gespecialiseerde bedrijven kunnen die belemmeringen worden overwonnen. Het volgens duidelijke normen uitbesteden van securitytaken aan derden, stelt alle

partijen in staat zich te richten op waar ze écht goed in zijn. Rendement op security-investeringen kan hierdoor verbeteren.

1.2.4 Inherente kwaliteit

Bij het adequaat laten functioneren van bedrijfsprocessen hoort het alert zijn op kansen en bedreigingen. Beschermende maatregelen zijn inherent, ook als het informatietechnologie betreft. Dit wordt niet altijd als vanzelfsprekend gezien. Toch zou deze kwaliteit niet aan een product of dienst moeten worden toegevoegd, maar daar juist een onlosmakelijk onderdeel van moeten zijn. Beveiliging en continuïteit mogen (of liever: moeten) beschouwd worden als onderdelen van het kwaliteitssysteem. In het ontwerpen, bouwen en beheren van informatiesystemen en -infrastructuren wordt informatiebeveiliging veelal als optie meegenomen. We denken nog te vaak in termen van ‘additioneel’; beveiliging wordt ‘toegevoegd’ in plaats van

‘ingebouwd’. Het wordt gezien als een ongewenst – want kostenverhogend – bijeffect. Continuïteit en beveiliging worden daarom vaak apart begroot en dus te gemakkelijk geschraapt of doorgeschoven naar de toekomst. Men concentreert zich veelal op perimeterbeveiliging; de bedreiging komt van buiten en daar moet wat tegen gedaan worden. De aandacht gaat hierbij vooral uit naar preventieve maatregelen, waarbij repressieve- en herstelmaatregelen onderbelicht blijven.

Meer dan airbags

De auto-industrie laat een analogo voorbeeld zien. Jaren geleden werd een auto puur gezien als transportmiddel. Wanneer er al sprake was van beveiligingsmaatregelen ging dat om niet meer dan bumpers, remlicht, richtingaanwijzer en deurslot. Perimeterbeveiliging dus. Dat was logisch, gezien het verkeersbeeld in die periode, de beperkte technologische



Figuur 2 Integrale benadering van security

mogelijkheden en het ontbreken van serieuze wet- en regelgeving. Fabrikanten als Volvo en Saab waren innovatief op het gebied van beveiliging maar slechts een selecte groep klanten was bereid ervoor te betalen.

Deze situatie is drastisch veranderd. Geen enkele fabrikant kan het zich nog veroorloven veiligheid en bescherming te negeren. De kans op een incident – botsing, inbraak, ontvreemding – is vele malen groter geworden en het schadebeeld is substantieel gegroeid. Zowel fabrikant als bestuurder wordt geconfronteerd met wet- en regelgeving op het gebied van verkeersveiligheid en -aansprakelijkheid. Ieder onderdeel van een auto wordt, naast de functionaliteit, bekeken op veiligheidsaspecten. Maatregelen als kreukelzones en kooiconstructie, brandwerende en antireflecterende materialen, veiligheidsgordel, rondom airbags, derde remlicht en tubeless banden zijn standaard in plaats van optioneel. Intelligentie ondersteunt de berijder bij beslissingen en grijpt in, zoals in het geval van adaptieve cruisecontrol en ESP, wanneer het mis dreigt te gaan. Er wordt zelfs met technische middelen gelet op de alertheid van de berijder.

Het onderhoud van deze veiligheidssystemen wordt overgelaten aan specialisten tijdens onderhoudsbeurten. Men is zich er nu terdege van bewust dat door de

omgevingsfactoren hogere eisen worden gesteld aan de berijder en dat hij niet onfeilbaar is. De bedreiging komt dus ook van binnenuit in de vorm van menselijk falen. Er is nu sprake van integrale beveiligingsmaatregelen. Bij het ontwerp worden deze aspecten meegenomen.

Hoge eisen

Vertalen we dit naar het bedrijfsleven dan zien we sterke overeenkomsten. We zijn ons meer bewust van de waarde van informatie. De schade bij imagooverlies en aansprakelijkheid na een calamiteit wordt duidelijker zichtbaar. Talloze voorbeelden van algemene en branchespecifieke wet- en regelgeving waar wij en onze klanten mee te maken hebben zijn voorhanden. In aanbestedingsprocedures worden hoge eisen gesteld aan leveranciers die het beheer krijgen over kritische bedrijfsinformatie. De complexiteit van informatiesystemen en beveiligingsopties is fors toegenomen en het ontbreekt aan kennis om deze goed te onderhouden. Beveiliging moet een integraal onderdeel zijn van ons denken, doen en handelen. Het moet ingebakken zijn in onze business-activiteiten. In de architectuur van bedrijfsprocessen hoort beveiliging te zijn opgenomen. Als dat goed gebeurt en beveiliging een organische eenheid vormt met de bedrijfsprocessen en -technieken, dan is het geen kostenpost meer, maar juist een business-enabler. Beveiliging maakt het dan mede mogelijk dat producten

en diensten de kwaliteit hebben c.q. krijgen die we wenselijk vinden.

Glurders en andere mensen

In de gangbare literatuur wordt kwaliteit van informatievoorziening gekenmerkt door: integriteit, betrouwbaarheid, beschikbaarheid, effectiviteit, efficiency en controleerbaarheid. De eerste drie aspecten hebben rechtstreeks met beveiliging en continuïteit te maken. Daarbij moet worden opgemerkt dat de keten zo sterk is als zijn zwakste schakel en dat geldt ook voor de samenhang in beveiligingsmaatregelen.

WE KUNNEN ECHTER NOG ZULKE MOOIE TECHNISCHE VOORZIENINGEN TREFFEN; ALS DE MENS ER SLORDIG MEE OMGAAT, HEBBEN ZE GEEN ZIN. ENKELE VOORBEELDEN:

- We kunnen nog zoveel back-ups maken, maar als we nooit testen of ze bruikbaar zijn, kan het zijn dat we niets meer hebben als het er op aan komt;
- Als we nooit het bestand van toegangs-gerechtigden schonen, dan moeten we niet gek opkijken als er onbevoegden toegang hebben tot onze bestanden, applicaties en gebouwen;
- Als we ons niet bewust zijn van de gevoeligheid van onze gegevens (ook op onze computer), kunnen ze zo bij de vuilnis terecht komen;

- Als we goede veiligheidsvoorzieningen op ons netwerk hebben, maar we staan toe dat er ongecontroleerd op ingelogd kan worden, kunnen de gevolgen desastreus zijn;
- Als we niet zo af en toe controleren op ongeautoriseerde draadloze verbindingen, kunnen we zomaar ‘gluurders’ op ons netwerk hebben.

1.2.5 Wat bedreigt ons?

We hebben het gehad over een veranderende wereld, het feit dat we onze kansen moeten grijpen en ons tegelijk moeten wapenen tegen bedreigingen. Maar waar bestaan die bedreigingen dan uit? Waar komen ze vandaan? Waartegen moeten we ons wapenen?

IN VERSCHILLENDE METHODEN WORDT GEREFEREERD AAN BEPAALDE INDELINGEN VAN BEDRIJVEN EN PROJECTEN. DIE INDELINGEN WORDEN NOGAL EENS AANGEDUID MET ACRONIEMEN:

- PIOFAH (Personeel, Informatie, Organisatie, Financiën, Apparatuur, Huisvesting);
- OPAFIT (Organisatie, Personeel, Apparatuur, Financiën, Informatie en Technologie);
- MAPGOOD. (Mensen, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving en Diensten (van derden)).

Maar welke indeling ook wordt gehanteerd, het is duidelijk dat snel we op al deze terreinen onze maatregelen moeten nemen om de bedrijfsprocessen onder alle omstandigheden te kunnen laten functioneren. En de balans van al die maatregelen moet ervoor zorgen dat er een evenwichtige verdeling is die alle schakels sterk houdt.

De riskante mens

Eén schakel willen we er uitlichten. Omdat we snel geneigd zijn om ons heil in de techniek te zoeken, vergeten we gemakkelijk de ‘ongrijpbare’ invloed van de mens. Meerdere onderzoeken hebben aangetoond dat het grootste gevaar dat ons bedreigt nog steeds de mens is. Het is vooral de mens die we in dienst hebben: de eigen medewerker, de vrijwilliger of de inhuurkracht!

De mens onderscheidt zich van een technisch middel in een aantal opzichten. Deze opzichten maken hem kwetsbaar en daarmee is hij een bron van risico's.

DE MENS

- is slordig;
- maakt fouten;
- is onderhevig aan stemmingswisselingen;
- is vatbaar voor tegenslagen;
- is omkoopbaar;
- heeft insiders-kennis;
- kan zich gepasseerd voelen;
- kan zorgen hebben;
- kan ontevreden zijn;
- heeft particuliere opvattingen over goed en kwaad;
- is onderhevig aan maatschappelijke opvattingen (zie ook hoofdstuk 3.3).
- et cetera

En zo kunnen we nog wel even doorgaan. Het is niet voor niets dat opvoeding, wet- en regelgeving en een systeem van controle- en strafmaatregelen er al sinds de Oudheid voor zorgen dat 'de mens' een beetje in het gareel blijft.

1.2.6 Levensstijl en kosten

Het menselijk lichaam besteedt onder normale omstandigheden ongeveer 10 procent van zijn energie aan het bestrijden van allerlei onheil, zoals virussen, bacteriën e.d. Een ongezonde levensstijl en een ouder wordend lichaam vragen meer energie en vaak oplopende kosten. Hygiëne, gezonde voeding, verstandige omgang met c.q. vermijding van gevaarlijke situaties en voldoende beweging kunnen veel gezondheidsschade tegengaan.

De vergelijking ligt voor de hand. Als we in de informatietechnologie niet 'gezond' leven en de gevaren niet zien of willen onderkennen, dan moeten we niet gek opkijken als we voor hoge kosten komen te staan. Ons bedrijf zou er zelfs aan kunnen 'overlijden'. Als we informatietechnologie omgeven met gezond gedrag en we voldoende intrinsieke maatregelen hebben ingebouwd bereiken we een gezond evenwicht.

Schattingen

Hoeveel procent van onze IT-uitgaven is gericht op het waarborgen van de continuïteit? Moeten we ongelimiteerd kosten maken om elke bedreiging te voorkomen? Nee! Dat doen we in het normale leven ook niet. We schatten onze kansen in. Doen voortdurend aan risicomanagement. We spreken zelfs al over de waarde van een mensenleven: hoeveel mag een operatie nog kosten? Moeten we een ongezond levende patiënt nog verzekeren? Laten we nuchter blijven: we investeren alleen maar als het ons iets oplevert en als we het ons kunnen veroorloven (of kunnen terugverdienen). Het beschermen van onze bedrijfsprocessen moet op dezelfde manier worden benaderd. Simpelweg: voorkomen is beter dan genezen.

1.3 VANZELFSPREKEND

1.3.1 Plezier?

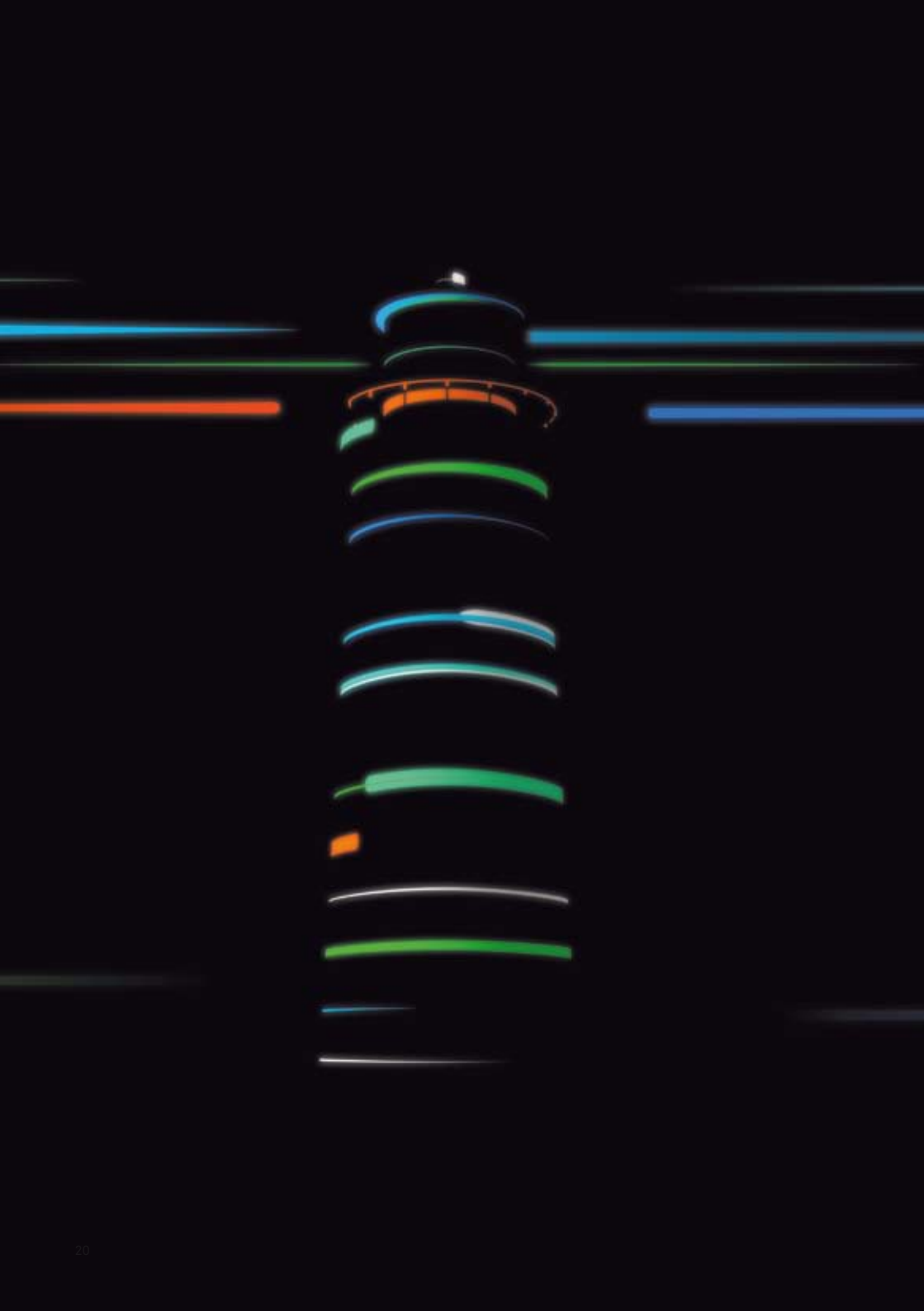
We kunnen het ons niet veroorloven om onzorgvuldig met kernprocessen om te gaan. Het beschermen ervan moet een vanzelfsprekend onderdeel zijn van onze kritische bedrijfsprocessen en alles wat die processen ondersteunt. Wordt het daarmee een plezierig, spannend onderwerp? Wellicht moeten we ons plezier halen uit het feit dat zaken ongehinderd voortgang vinden, juist doordat we er zorgvuldig mee zijn omgegaan (en daarmee de concurrentie de loef afsteken!).

Wordt de Security manager of de Business Continuity manager daarmee een graag geziene gast? Op zijn minst wordt hij/zij een vanzelfsprekende partner die ongehinderde voortgang mede mogelijk te maakt.

1.3.2 In control

Deze uitgave van Getronics behandelt aan de hand van een model een aantal onderwerpen die met Business Continuity Management annex informatiebeveiliging⁴ te maken hebben. Het model laat zien wat er allemaal nodig is om als directie te kunnen zeggen: ik ben 'in control', ik beheers mijn bedrijfsprocessen, ik weet dat het goed gaat en ik weet ook waar ik nog kan verbeteren. Is het model daarin compleet? Nee, dat kan niet. Maar het geeft wel een beeld van de verschillende invalshoeken van waaruit de problematiek kan worden bekeken. ←

4. De begrippen Business Continuity Management (BCM) en informatiebeveiliging of security worden in deze uitgave door elkaar gebruikt. Het vakgebied is nog te onvolwassen om eenduidigheid in begrippen te hebben. De school die voortkomt uit het BCM-denken redeneert vanuit bedrijfsprocessen en beschouwt informatiebeveiliging of security als een van de onderwerpen die continuïteit van de business mogelijk maken. De school die opgegroeid is met informatiebeveiliging c.q. security komt vanuit de informatietechnologie en deelt security in in de drie eerder genoemde begrippen vertrouwelijkheid, integriteit en beschikbaarheid (continuïteit). Continuïteit is daarmee een onderdeel van security geworden en daarmee weer een onderdeel van de kwaliteit van bedrijfsprocessen. We laten ons hier niet verleiden tot een semantische discussie. De context waarin de begrippen in dit boekje worden gebruikt zal duidelijk maken wat we bedoelen.

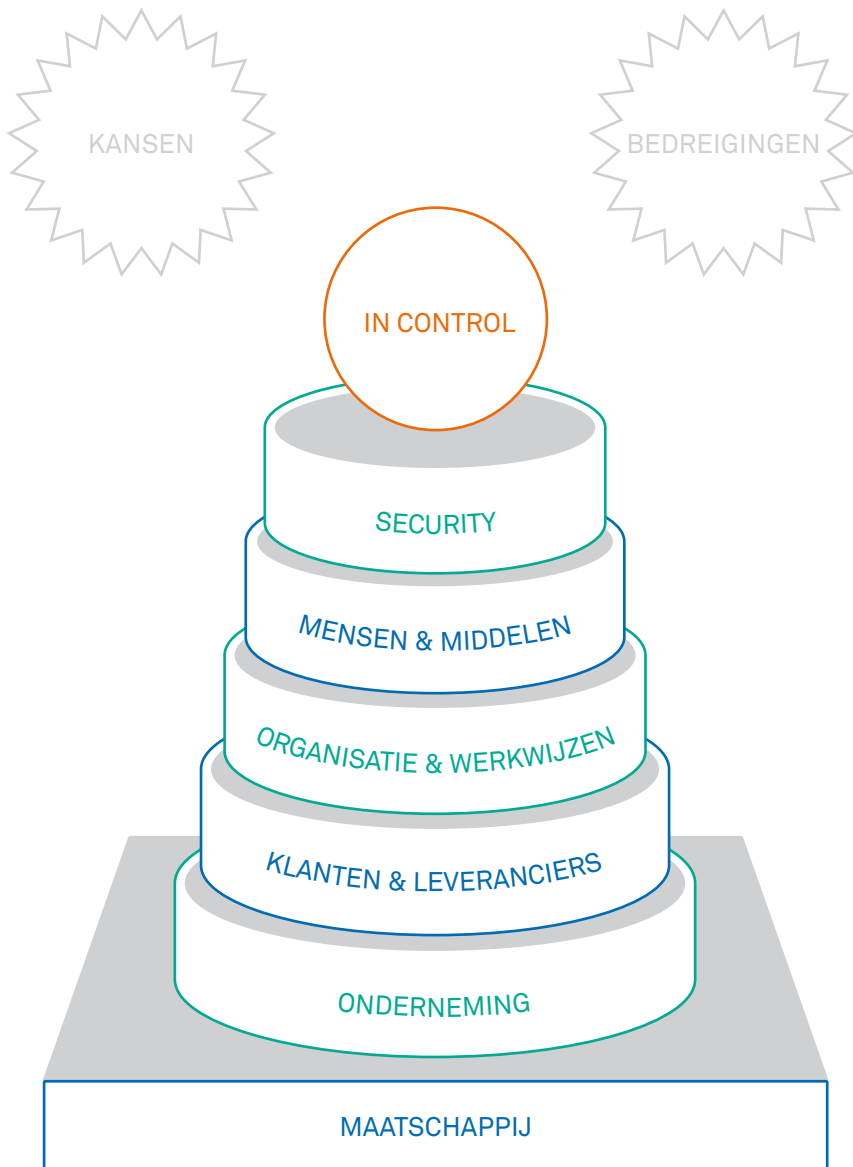


2 DE TOREN

2.1 HET MODEL

IEDEREEN IS ERMEE OPGEGROEID. MET ONZE ONHANDIGE VINGERTJES MOESTEN WE DE SCHIJVEN IN DE JUISTE VOLGORDE OP ELKAAR STAPELEN. EEN STABIELE ONDERGROND WAS EEN VEREISTE, WILDE ALLES OP ZIJN PLAATS BLIJVEN. TOT SLOT MOEST HET DOPJE BOVENOP GOED WORDEN AANGEDRUKT, ANDERS KON JE ER NIET MEE WEGLOPEN: DE KANS DAT ALLES VAN 'Z'N STOKJE' GLEED WAS GROOT. DEZE ANALOGIE HEBBEN WE GEBRUIKT OM DE SAMENHANG TE TONEN TUSSEN DE ONDERWERPEN WAARMEE HET BESTUUR VAN EEN ONDERNEMING TE MAKEN HEEFT, ALVORENS HET KAN ZEGGEN:

IK BEN - IN CONTROL - MIJN ONDERNEMING
HEEFT VOOR MIJ GEEN GEHEIMEN MEER
EN IK WEET WAAR IK AAN TOE BEN.



Figuur 3 De toren

Alles op zijn plaats

Beschouw de onderneming (bedrijf, overheidsorganisatie, etc.) als de onderste schijf en de kern van deze schijventoren. Geworteld in de maatschappij (de ondergrond), levert zij diensten en/of producten aan klanten en ontvangt zij producten en of diensten van haar leveranciers of werkt daarmee samen in ketens: de tweede schijf.

Om efficiënt en effectief te kunnen werken is het nodig dat de onderneming geordend is en werkt volgens afspraken en (werk)processen: de derde schijf.

De vierde schijf geeft de mensen en middelen weer die nodig zijn om de bedrijfsprocessen gaande te houden, te innoveren en te beheren. Hiertoe behoren uiteraard de medewerkers en de ingehuurde krachten, maar ook de informatietechnologie, de al dan niet door computers via het internet aangestuurde productiemachines en de kassa's op de balies.

Schijf nummer vijf symboliseert de beveiliging. Alle maatregelen die genomen worden om continuïteit in welke vorm dan ook te waarborgen en de kwaliteit van de dienstverlening te verzekeren, behoren tot het domein van deze schijf.

Ten slotte geeft de afsluitende dop weer dat alles op zijn plaats zit. Als de dop is aangebracht, u kunt zeggen: ik ben 'in control'.

2.2 VALLEN

Zoals gezegd, de samenhang en de volgorde van deze toren zijn belangrijk. De schijven hebben een zekere hiërarchie, een bepaalde volgorde en alleen alle schakels tezamen vormen een toren die een geheel van samenhangende processen symboliseert.

Een toren waarin een schijf ontbreekt, mag dan wel op een toren lijken, maar is het niet. Een toren waarvan de dop ontbreekt, kan heel lang blijven staan, totdat de kansen of bedreigingen het model zo opschudden dat stukken eruit vallen en de toren geen stabiele toren meer is.

Wilt u uiteindelijk kunnen zeggen dat alles onder controle is, dan moeten de stukken passen en compleet zijn. Het is een onlosmakelijk geheel en daarmee afhankelijk van al zijn onderdelen. Een onderneming bereikt pas haar doel en is daarin concurrerend als het geheel 'past' en aantoonbaar samenhang vertoont.

Het goed functioneren van de schijven wordt gewaarborgd door de maatregelen van security. Eerder legden we al uit dat dit bestaat uit de elementen 'beschikbaarheid', 'vertrouwelijkheid' en 'integriteit'. Dit schijfje is kleiner dan de andere. Security vormt een van de randvoorwaarden om kwalitatief goede dienstverlening en producten aan te bieden. En net zoals de andere schijven vormt het geheel pas een sterke toren als security er een geïntegreerd onderdeel van is.

2.3 SCHUDDEN EN KANTELEN

Een onderneming, gesymboliseerd door de toren, kent invloeden van binnenuit en van buitenaf. Er is dynamiek in de mogelijkheden en de kansen, evenals in de dreigingen en de gevaren. Elke manager vraagt zich wel eens af: hoe weet ik nu zeker dat ik het geheel in handen heb, dat ik 'in control' ben?

Met de dop op deze toren kan het geheel een stootje hebben. Je kunt schudden en kantelen. De toren kan zelfs vallen. Maar de dop zorgt ervoor dat het een geheel blijft. Het is en blijft 'in control'. De dop moet zelfs een beetje knellen, zodat niet bij de eerste de beste beweging de schijven eraf vallen.

De toren staat ergens op; een onderneming staat in de maatschappij. Zij vindt daarin haar bestaan en is onderhevig aan de in die maatschappij heersende wet- en regelgeving, normen en standaarden. Ook de maatschappij is een dynamisch geheel, zij ontwikkelt zich en past zich aan. Een onderneming die niet op tijd mee verandert, mist de boot en verliest terrein. Bovendien is de maatschappij breed. Sommige ondernemingen hebben te maken met meerdere 'maatschappijen'. Ondernemingen die in

meer dan één land of continent opereren, zien de uitdaging van meerdere stelsels van wet- en regelgeving en van verschillende normen en standaarden.

Altijd verandering

De enige en blijvende constante is verandering. De maatschappij verandert, de inhoud van de verschillende 'schijven' verandert: alles is voortdurend in beweging. Wil een onderneming overleven dan moet zij voortdurend alert zijn op deze veranderingen en daarop inspelen. Wil ze dan ook nog verantwoording kunnen afleggen van de business-as-usual, dan ligt hier de uitdaging voor Business Continuity Management.

BUSINESS CONTINUITY MANAGEMENT (BCM) KENT EEN VEELOMVATTENDE DEFINITIE.

HET IS EEN HOLISTISCH MANAGEMENTPROCES DAT:

- potentiële bedreigingen (en kansen!) van een organisatie identificeert;
- de impact van die dreigingen (als ze daadwerkelijk optreden) voor het functioneren van een organisatie vaststelt;
- voorziet in een framework voor het bouwen van organisatorische veerkracht;
- voldoende antwoord geeft op die bedreigingen en daarmee de belangen van zijn stakeholders, reputatie, merk en waardebepalende activiteiten voor de lange termijn veiligstelt.

De onderneming die kan aantonen dat dit goed georganiseerd, aantoonbaar werkend en geborgd is voor de lange termijn, is daadwerkelijk 'in control'. ←



3 KLANTEN EN LEVERANCIERS

3.1 DIFFUSE GRENZEN

Een onderneming is afhankelijk van haar klanten aan de ene kant en van haar leveranciers aan de andere kant. Zo was het althans tot voor kort. Er kwam iets binnen, daar deden we wat mee, we verkochten het weer en het ging naar buiten. De grenzen van elke onderneming waren bepaald. Je kon ze aanwijzen en het onderscheid tussen de domeinen was helder. Dat is nu niet meer zo. Klanten hebben toegang gekregen tot de 'backoffice', en ze beïnvloeden bedrijfsprocessen door hun individuele voorkeuren online bekend te maken, orders te volgen en gegevens te wijzigen. Dat is de ene kant. En aan de andere kant van de onderneming hadden we de leverancier. Maar die is nu ketenpartner en zorgt samen met anderen in de keten (ook de partijen die hij weer in zijn netwerk heeft) voor een samenhangend netwerk dat uiteindelijk

moet uitmonden in een dienst of product waar de tot in de backoffice doorgedrongen klant om gevraagd heeft. Dat samenhangende netwerk kan overigens per aangeboden dienst of product wisselen, want de relaties duren korter en zijn gemakkelijker inwisselbaar. Het ene moment bent u partner en in een andere samenstelling bent u concurrent.

Wie vertrouwt u?

Gezien vanuit continuïteitsperspectief: hebt u in de hand wat 'vreemde elementen' op uw netwerk uitvoeren? Kan iemand op uw netwerk inbreken of rondsnuffelen? Hoe zit het met de partij waaraan u uw ICT heeft toevertrouwd?

Het is belangrijk voor een onderneming 'in control' om haar – letterlijke en figuurlijke – netwerk te kennen en te kunnen controleren. De onderneming moet precies weten welke veranderingen er zijn, wat die inhouden en welke kansen en bedreigingen

ze met zich meebrengen. Het is voor een klant vaak lastig om te achterhalen bij wie hij in een organisatie moet zijn voor een klacht. De onderneming die het netwerk niet kent, gaat uiteindelijk ten onder tussen kastje en muur.

3.2 DIT WAS (NIET) DE AFSPRAAK

Afspraken die ondernemingen onderling maken, worden vastgelegd in contracten. Daaronder liggen vaak afsprakendossiers en dienstverleningsovereenkomsten.

Deze sets van afspraken weerspiegelen onder andere verantwoordelijkheden, verwachtingen, aansprakelijkheden, rapportageverplichtingen en bijvoorbeeld geschillenprotocollen.

Een onderneming die 'in control' wil zijn, moet kunnen vertrouwen op de gemaakte afspraken en op haar beurt garant staan voor de verplichtingen die daar bij horen. Actief management van deze afspraken en het voortdurend monitoren of gemaakte afspraken passen binnen de ondernemingsstructuur en wijze van werken zijn nodig om de bedrijfscontinuïteit te waarborgen. Verkeerde inkoop, onvolgende of onevenwichtige menskracht of productiecapaciteit kunnen leiden tot verlies, stagnatie, schadeclaims of een forse inbreuk op het zorgvuldig opgebouwde publieke imago.

Heldere afbakening

Gezien de maatschappelijke hang naar deregulering en de vaak kortdurende relaties tussen bedrijven, wordt de vraag naar zo dun mogelijke contracten en afsprakendossiers steeds luider. Toch ontkomen we er niet aan dat we, daar waar we voor onze bedrijfsprocessen 'in control' willen zijn, ook duidelijk moeten kunnen maken hoe ver die control of beheersing zich uitstrekt. Met andere woorden, de scope waarbinnen we ons bewegen, moet duidelijk zijn. Het maakt een duidelijke afbakening van verantwoordelijkheden en heldere kaders noodzakelijk.

Het kunnen afleggen van verantwoording is belangrijk, maar ook het inrichten van een behoorlijk autorisatie- en authenticatiemechanisme (identificatie). Daarnaast is een escalatiemogelijkheid van groot belang, bijvoorbeeld om te weten wat van u wordt verwacht als de zaken anders lopen dan gepland. Om te kunnen acteren als bedrijfsonderdelen stagneren door incidenten en calamiteiten. U wilt toch weten wat u moet doen als er bij een leverancier iets gebeurt waardoor leverantie aan u in gevaar komt?

3.3 DE MENS, DE NORM EN DE WAARDE

De mens als zwakke schakel is al even genoemd. Die mens heeft persoonlijke opvattingen over goed en kwaad en is ook

onderhevig aan de publieke moraal. Wat betekenen al die maatschappelijk en private normen en waarden in samenhang met continuïteit en beveiliging? Wat is de impact van bijvoorbeeld:

- de verharding van de maatschappij?
- de 'job-hopping' cultuur?
- de morele elektronische afstand?

3.3.1 Verharding

Elektronische wapenwedloop

In korte tijd zijn we gewend geraakt aan termen als virussen, SPAM, spyware, phishing, hackers en crackers. Het internet heeft niet alleen ons maar ook de criminele wereld ongekende mogelijkheden gegeven. Om een bedrijf binnen te komen, hoeven we ons huis niet meer uit. We hebben de middelen gecreëerd om ons te wapenen. De wapenwedloop is in elektronische zin nog maar net begonnen.

Miljarden euro's gaan om in het grijze, criminele en vooral elektronische circuit van SPAM, spyware en (identiteits)fraude. De oorspronkelijke hacker was nog idealistisch bezig, namelijk met het aantonen van beveiligingslekken. Zijn opvolger verdient grote sommen geld met het daadwerkelijk verstoren van bedrijfsprocessen en het gijzelen, stelen en vervalsen van gegevens. En lukt het niet elektronisch, dan wordt toevlucht gezocht tot social engineering. Wetgeving en justitie staan nog vaak machteloos tegenover elektronische misdaad.

En laten we niet vergeten dat de eigen medewerker ook deel uitmaakt van de veranderende maatschappij. Loyaliteit aan werkgevers is de laatste decennia afgenomen. Veel bedreigingen van ondernemingen komen van binnenuit. Variërend van 'gewone fouten' tot bewuste fraude en afpersing komen ze in alle bedrijven voor. Bovendien is de goedwillende medewerker zich vaak niet voldoende bewust van de risico's die zijn – soms naïeve – gedrag met zich meebrengt, zowel voor het bedrijf als voor de medewerker persoonlijk.

3.3.2 Jobhopping

Wie blijft?

De binding met een bedrijf en de daarbij horende loyaliteit nemen af. We 'hoppen' gemakkelijk van de ene naar de andere baan (in- of extern). Dat veroorzaakt een sterke doorstroming en wisseling van – mogelijk vitale – kennis. De morele afstand tussen onderneming/bedrijfsproces en medewerker wordt groter. Het moderne flexibele arbeids- en ontslagrecht draagt daar mogelijk aan bij. Loyaliteit ('mijn medewerkers doen zoiets niet') is niet meer iets waarop kan worden gerekend. De omvang van een bedrijf heeft daar ook mee te maken. Naarmate de eigen bijdrage aan het eindresultaat van de onderneming kleiner wordt, is de betrokkenheid van de medewerkers minder. Het delen van kennis en een

HET VERTROUWEN DAT WE HEBBEN IN ONZE KETENPARTNERS OVER DE CONTINUÏTEIT VAN LEVERING KAN ZOMAAR VERDWIJNEN DOOR HET VERTREK VAN EEN PAAR KEYPLAYERS.

zorgvuldige afweging van de gebieden waar de medewerkers toegang toe hebben, wordt in een cultuur waar mensen snel van positie wisselen en/of de loyaliteit gering is, erg belangrijk. De continuïteit van bedrijfsprocessen kan ervan afhankelijk zijn.

Overigens komt jobhoppen ook voor bij onze ketenpartners. Het vertrouwen dat we hebben in onze ketenpartners over de continuïteit van levering kan zomaar verdwijnen door het vertrek van een paar keyplayers.

3.3.3 Morele afstand

We hebben het over een begrip dat nog niet goed doordacht is, maar dat alles te maken heeft met het 'mijn en dijn' in de virtuele wereld. In de fysieke wereld zitten we dicht op ons bezit. Een ladekast op mijn kamer is iets anders dan een map of een folder in een librarystructuur op een server 'ergens' op deze wereld. De virtuele afstand tussen mij en mijn gegevens doet

ook iets met mijn begrip van 'dit is van mij en daar heb ik voor te zorgen'. In onze afweging van risico's en te nemen maatregelen is dit een niet te onderschatten factor.

3.4 VERTROUWEN EN CONTROLE

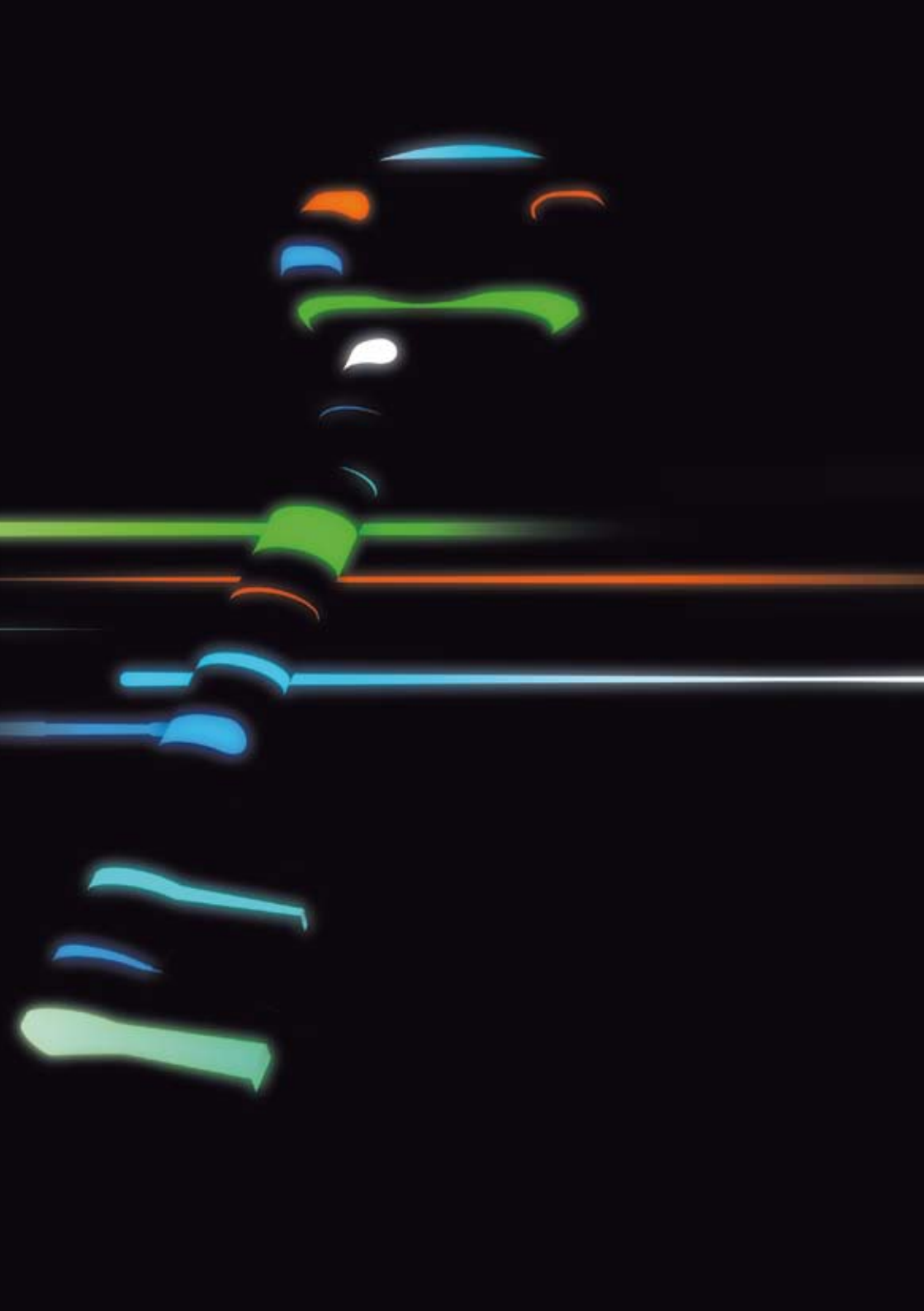
Vertrouwen is goed, controle is beter. Menig accountant en IT-auditor heeft dit tijdens zijn of haar opleiding geleerd en zelf in de mond genomen.

Maar hoeveel outsourcingcontracten zouden er gesloten zijn zonder verdere bepalingen over de beveiliging van de gegevens? Vaak wordt de verantwoordelijkheid hiervoor overgeheveld van de ene partij naar de andere, zonder expliciete afspraken. Security en continuity vormen bij veel partijen geen vanzelfsprekende dienstverlening. Garantie op deze gebieden? Wie durft het te geven? Toch gaat het gebeuren.

Geen zorgen

De eerste bedrijven, waaronder Getronics, durven nu garanties te geven op bijvoorbeeld de managed infrastructures en op mailwashing en continuïteit. Klanten hoeven zich daarover geen zorgen meer te maken. Zijn ze daarmee van hun verantwoordelijkheden af richting klanten en maatschappij? Nee, zeker niet, maar via allerlei 'in control'-constructies zijn zekerheden te verkrijgen die voldoende zijn om die gewenste verantwoording te kunnen afleggen. Via een managementmechanisme van afspraken, controles en verslaglegging moeten bedrijven die een afhankelijkheidsrelatie met elkaar hebben hun maatregelen en controlesystemen op elkaar afstemmen. 'Vertrouwen is goed, controle is beter' geldt ook in ketenrelaties.





4 MAATREGELEN IN DE JUISTE PROPORTIE

EEN ORGANISATIE MOET ZO ZIJN INGERICHT DAT ER EEN OPTIMALE ALERTHEID IS OP DE KANSEN EN BEDREIGINGEN DIE VAN BINNENUIT ÉN VANUIT DE OMGEVING KOMEN. NAGENOEG ELK BEDRIJF HEEFT DE CONTINUÏTEIT VAN DE BEDRIJFSVOERING HOOG IN HET VAANDEL STAAN. MAAR DE MANIER WAAROP ERMEE WORDT OMGEGAAN VERSCHILT PER SECTOR, BEDRIJFSOMVANG, ET CETERA. DREIGINGEN EN POTENTIËLE VATBAARHEID VOOR DIE DREIGINGEN KUNNEN VOOR VOOR VERSCHILLENDE ORGANISATIES IDENTIEK ZIJN; DAT ZEGT NOG NIETS OVER DE OMVANG VAN HET RISICO EN DE MOGELIJKE GEVOLGEN.

De schade die het gevolg is van een incident verschilt ook per bedrijf. Een soortgelijk incident kan bij een internationale bank heel andere proporties hebben dan bij een MKB-bedrijf. De maatregelen die per bedrijf genomen worden, kunnen dan ook uiteenlopend zijn in omvang en kosten. Wat zijn de juiste proporties?

4.1 KOSTEN EN BATEN

Een gezond en stabiel bedrijf is in staat om organisatorisch, technisch én ook fysiek zijn bedrijfsprocessen te beschermen. Hoe een organisatie wordt ingericht en werkt, wordt medebepaald door de producten en diensten die het bedrijf levert. Klanten en leveranciers zijn eveneens van invloed op de manier van organiseren en werken. Dat geldt des te sterker als wordt gewerkt in afhankelijkheid van ketens.

Alle elementaire zaken (functies, hiërarchie, procedures, richtlijnen, werkinstructies, controlemechanismen en rapportages) spelen een rol bij het onder controle krijgen van risico's, evenals het technisch en organisatorisch (procedureel) beleid. Automatisch dupliceren van transacties op een extern ondergebrachte standby-omgeving en een goed ingevoerde functiescheiding zijn hier voorbeelden van.

Zelfkennis

Een risicoanalyse en een kostenbatenanalyse helpen bij het bepalen van investeringen in continuïteits- en beveiligingsmaatregelen. Tegen welke risico's wil ik mij beschermen? Hoe groot is de kans dat ik ermee word geconfronteerd? Wat gaat het kosten als er iets gebeurt en welk bedrag wil ik maximaal investeren om me ertegen te beschermen? Als we iets verder kijken, blijkt het vaststellen van de kosten ingewikkelder dan het op het eerste gezicht lijkt. Het begrip 'kosten' kan immers breder worden uitgelegd dan in termen van geld. We hebben het niet alleen over kosten als gevolg van directe schade; we hebben mogelijk ook te maken met de gevolgen van het niet meer kunnen voldoen aan wet- en regelgeving, imagoschade, claims, proceskosten en het mogelijk niet kunnen afleggen van maatschappelijke verantwoording.

Een organisatie die zichzelf kent en hierin bewuste keuzes maakt, heeft een belangrijke stap gezet in het onder controle krijgen van haar bedrijfsvoering.

4.2 DE STRUCTUUR

Om een op continuïteit gerichte bedrijfsvoering te bereiken, moeten alle lagen van een onderneming gericht zijn op kwaliteit. De aandacht hiervoor moet zowel op strategisch, op tactisch en als op operationeel niveau verzekerd zijn, en de motivatie moet voortkomen uit de wens om kwalitatief goede producten en diensten te leveren. Toch wijst de praktijk uit dat het invoeren van maatregelen die de continuïteit en de beveiliging van de onderneming moeten waarborgen, pas worden genomen als bijvoorbeeld wet- en regelgeving of een negatieve accountantsverklaring daartoe dwingen.

Voordat een organisatie begint met het opzetten van een structuur die het beschermen van bedrijfsprocessen garandeert, is het belangrijk dat de juiste beleidsuitgangspunten zijn geformuleerd. Het management formuleert in deze uitgangspunten de belangen die moeten worden beschermd. Dit vormt immers de basis voor de diepgang en de detaillering van te nemen maatregelen.

EEN ORGANISATIE DIE ZICHZELF KENT EN HIERIN
BEWUSTE KEUZES MAAKT, HEEFT EEN
BELANGRIJKE STAP GEZET IN HET ONDER
CONTROLE KRIJGEN VAN HAAR BEDRIJFSVOERING.

Primaire waarde

Een procesanalyse haalt boven tafel welke bedrijfsonderdelen en -processen de primaire waarde vertegenwoordigen voor de organisatie. Een procesanalyse stelt ook vast hoe afhankelijk het bedrijf is van bepaalde processen en in welke mate het hierdoor kwetsbaar is. Wat zijn de single points of failure en waar zitten de zwakke, niet-redundante schakels? Op basis van de beleidsuitgangspunten wordt vastgesteld welke vervolgacties nodig zijn. Om efficiënt en eenduidig met deze vervolgacties om te gaan, is het verstandig de resultaten van de verschillende procesanalyses zoveel mogelijk te consolideren.

Als we inzicht hebben in een complete set van maatregelen die genomen moeten worden om de processen te optimaliseren of de risico's weg te nemen, wordt een implementatietraject gestart. De gevolgen van een geoptimaliseerd proces zijn terug te vinden in de onderliggende werk-instructies. Om nieuw geconstateerde risico's weg te nemen, kan het noodzakelijk zijn verdere initiatieven te ontplooiën, bijvoorbeeld om bepaalde informatiebeveiligingsmaatregelen te implementeren, afspraken met een derde partij te maken over disaster recovery of om de huidige wijze van functiescheiding te herzien.

Meer ogen

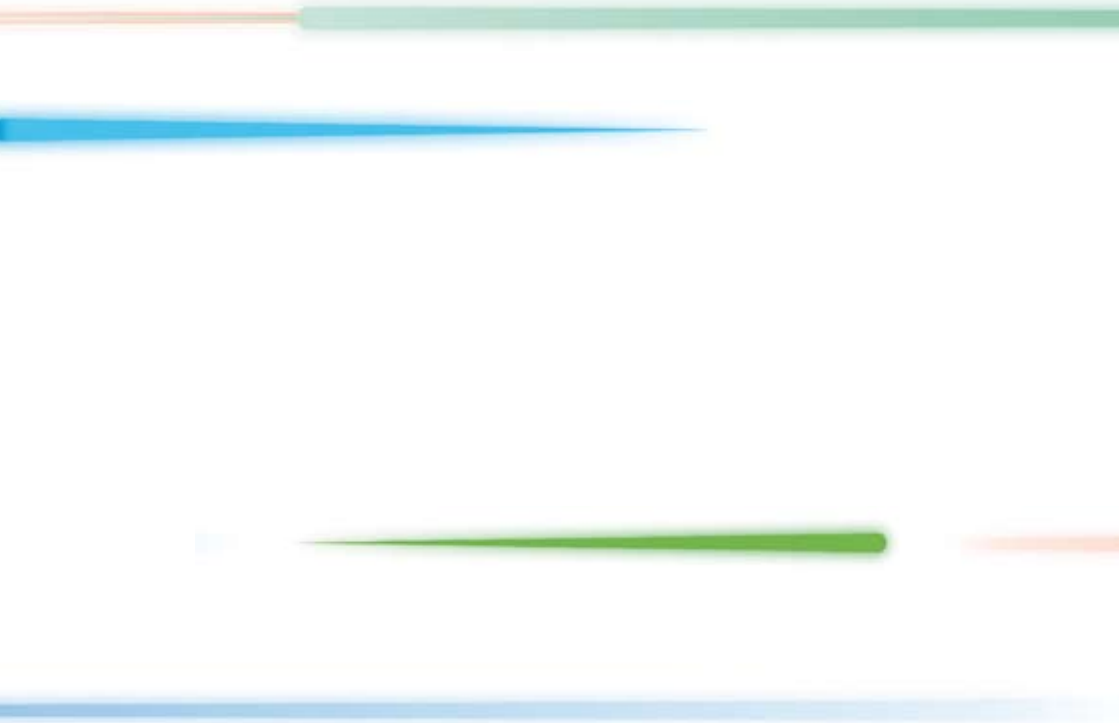
Functiescheiding is een klassieke manier van organisatorische beveiliging. Door de rechten van een individu te beperken, wordt voorkomen dat kwaadwillende medewerkers te veel schade aan kunnen richten. Automatiseringstechnieken hebben deze manier van organiseren een extra dimensie gegeven. Het komt nogal eens voor dat functiescheidingen worden doorbroken door een niet goed ingevoerde rechtenstructuur in autorisatieschema's. Het 'meer-ogen-principe' dient organisatorisch en technisch controleerbaar te zijn verwezenlijkt.

4.3 ZWAKKE SCHAKELS

Het komt regelmatig voor dat technische oplossingen de schuld krijgen van inefficiëntie en vertragingen, maar dat de mens binnen de structuur een van de zwakste schakels is, is een gegeven. Systematische aandacht voor bewustwording en voor technieken die zowel faciliteren als beschermen, zonder overbodige beperkingen op te leggen, maken deze schakel zo sterk mogelijk.

‘WIJ WETEN ALLEMAAL ELKAARS WACHTWOORD,
ZODAT WE GEMAKKELIJK BIJ ELKAARS
BESTANDEN KUNNEN, OF EVEN IETS KUNNEN
REGELEN ALS EEN COLLEGA NIET AANWEZIG IS.
IK STA VOOR IEDEREEN OP MIJN AFDELING IN.’

Herkent u deze praktijk? Een goede controle- en rapportagestructuur is van groot belang. Als de juiste besturingsorganen niet voorzien worden van de juiste informatie om te kunnen bijsturen, ontbreekt de noodzakelijke controle, waardoor geen verantwoording kan worden afgelegd. Functio-nerings- en beoordelingsgesprekken worden in steeds meer bedrijven gebruikt om medewerkers aan te spreken op het zorgvuldig omgaan met beveiligingsmaatregelen. ←



5 MENSEN EN MIDDELEN

MEDEWERKERS EN MIDDELEN: ZE KUNNEN ZOWEL KANSEN ALS BEDREI- GINGEN ZIJN. HET GAAT EROM ZE OP DE JUISTE WIJZE IN TE ZETTEN. IEDERE ONDERNEMER ZIET GRAAG DAT DE MEDEWERKERS ER ZIN IN HEBBEN. OP DIE MANIER WORDT DE VOLLEDIGE POTENTIE VAN HET BEDRIJF BENUT OM EEN GEZONDE BEDRIJFSVOERING TE REALISEREN EN TOONAANGEVEND TE ZIJN BINNEN DE BRANCHE. MEDEWER- KERS MOETEN DAARVOOR WEL GOED WORDEN GEFACILITEERD.

5.1.1 Personeelwisseling

Elk bedrijf heeft te maken met een wisselend personeelsbestand (zie ook hoofdstuk 3.3). Zeker als het bedrijf opereert in een specialistische branche, is de wereld klein en de kans groot dat een medewerker bij op een dag bij de concurrent aan de slag gaat. Daarom is het van groot belang om vooraf met de werknemer duidelijke afspraken te

maken over de manier waarop wordt omgegaan met bestaande klantcontacten en het bezit van bedrijfsgegevens.

Systeembeheerders

Een bijzondere groep medewerkers zijn de systeembeheerders. Zij zijn verant- woordelijk voor het onderhoud van de servers met bedrijfsinformatie. Over het algemeen zijn zij in staat om buiten applicatieve beperkingen toegang te krijgen tot deze informatie. Gelukkig neemt het aantal technische mogelijkheden toe om ook deze categorie medewerkers slechts gecontroleerde toegang te verlenen, maar het nemen van extra (ook organisatorische) maatregelen kan geen kwaad. Screeningen, geheimhoudings- verklaringen en contractuele bepalingen zijn wel het minste. Controlemaatregelen die onomstotelijk vaststellen welke handelingen door de beheerders zijn gedaan, horen daar zeker bij.

5.1.2 Opleiding en bewustwording

De noodzaak om de kennis en kunde van het bedrijf mee te laten groeien met de marktontwikkelingen, is de belangrijkste reden om mensen bij te scholen. Bovendien draagt scholing bij aan het voorkomen van verkeerd gebruik van bedrijfsmiddelen. Een medewerker die exact weet hoe en waarom hij een applicatie moet bedienen of een server beheren, werkt niet alleen efficiënter, maar zal ook minder snel een fout maken die nadelige gevolgen heeft voor de bedrijfsvoering.

'Onmisbare' personen

Het op een optimale manier intern coachen en scholen van medewerkers kan ertoe bijdragen dat teams minder afhankelijk worden van sleutelpersonen. Elke afdeling heeft wel een of meerdere onmisbaar geachte werknemers, oftewel werknemers die belangrijke kennis bezitten doordat ze langer in dienst zijn, betere scholing hebben genoten of meer

initiatief tonen dan hun collega's.

De rol van zulke medewerkers wordt vaak in de loop van de jaren steeds verder versterkt, omdat, gezien hun positie, steeds meer ontwikkelingen en wijzigingen via hen verlopen. Op het moment zelf lijkt dat dan vaak de snelste en beste oplossing, maar als zo'n medewerker plotseling wegvalt, ontstaat een moeilijk te overbruggen gat, dat een serieuze bedreiging kan vormen voor de continuïteit van bedrijfsprocessen.

Het spreiden van kennis binnen een team voorkomt dat een team te afhankelijk wordt van individuen. Eén oplossing is om periodiek werk te laten rouleren. Daarmee neemt tevens de kans op fraude door een enkele medewerker af, omdat het risico van ontdekking veel groter wordt.

Een vorig hoofdstuk wees er al op om medewerkers geregeld te doordringen van het nut en de noodzaak van beveiligings- en continuïteitsmaatregelen. Bewustwording

ALS ZO'N ONMISBARE MEDEWERKER WEGVALT, ONTSTAAT EEN MOEILIK TE OVERBRUGGEN GAT, DAT EEN SERIEUZE BEDREIGING KAN VORMEN VOOR DE CONTINUÏTEIT VAN BEDRIJFSPROCESSEN.

is een belangrijke preventieve factor. Maar dat besef moet worden onderhouden: veiligheidsmaatregelen zijn snel uit het bewustzijn verdwenen en behoren vaak niet tot het standaardhandelen van de medewerkers. Het is niet voor niets dat vrijwel elke norm en standaard op dit gebied hier aandacht voor vraagt. Een jaarplan voor communicatie rondom dit onderwerp is volgens sommige normen zelfs vereist.

5.1.3 Menselijk falen

Omvangrijke calamiteiten zijn vaak terug te voeren op menselijk falen. Maar medewerkers zijn niet de meest voorspelbare en betrouwbare bedrijfsmiddelen. Als we spreken over continuïteit en beveiliging van bedrijfsprocessen en informatievoorziening moeten we daar rekening mee houden. 'De grootste dreiging komt van binnenuit': dat geldt voor elk bedrijf. Voor een deel gaat het om opzettelijk gedrag, maar daarnaast is het simpelweg een kwestie van fouten maken.

Hoge werkdruk is meer regel dan uitzondering. En hoge werkdruk leidt ertoe dat maatregelen die in de ogen van medewerkers niet direct bijdragen tot productiviteit eveneens onder druk staan. Continuïteit- of beveiligingsmaatregelen en -procedures behoren al snel tot deze categorie.

Collegiale toetsing

Voor de continuïteit en veiligheid van kritische bedrijfsprocessen (en de medewerkers zelf), is het van groot belang medewerkers tegen zichzelf te beschermen. ICT- en andere processen zouden zo moeten worden ingericht dat handelingen pas kunnen worden afgerond na collegiale (of hiërarchische) toetsing. Zo wordt voorkomen dat een medewerker te grote schade kan aanrichten. Ook hier moet het 'meer-ogen-principe' zijn ingevoerd.

5.1.4 Misbruik

Medewerkers kunnen bewust misbruik maken van de mogelijkheden die hun functies bieden, bijvoorbeeld om zichzelf te verrijken. Om dat te voorkomen moeten gangbare maatregelen uit niet-gedigitaliseerde omgevingen worden doorgetrokken naar een ICT-omgeving. Is slechts een beperkte groep medewerkers geautoriseerd om producten bij een bepaalde leverancier te bestellen, dan dient de toegang tot de inkoopssystemen goed beschermd te zijn. Deze medewerkers mogen geen toegang krijgen tot digitale identiteiten die een bestelling kunnen goedkeuren, de aflevering bevestigen en de betaling van de factuur uitvoeren.

Wie controleert de beheerder?

Binnen geautomatiseerde financiële administraties is die beveiliging doorgaans wel geregeld, maar als we kijken naar beheerafdelingen, dan is het met de

waarborging over het algemeen minder goed gesteld. De rechten die medewerkers van een automatiseringsafdeling van bedrijfskritische systemen toebedeeld krijgen, kennen lang niet altijd voldoende beperkingen. En de controlemechanismen die mede dienen om de handelingen van een beheerder vast te leggen en te controleren – als dergelijke mechanismen aanwezig zijn – worden vaak onderhouden door dezelfde medewerker. Verantwoordelijkheden moeten hier op een goede manier worden gescheiden naar functie en rol.

Potentiële daders

Een onderzoek⁶ naar 150 gevallen van computermisbruik door eigen medewerkers leverde een zevental interessante observaties op.

1. De meeste medewerkers hadden aanwijsbare persoonlijke problemen die bijdroegen tot het verrichten van hun ongewenste handelingen, zoals paniek, alcohol- of drugsverslaving, medicijngebruik, persoonlijke problemen. Achteraf bleek dat omstanders niet verbaasd waren.
2. De betrokken medewerkers kampten met ontevredenheid die te wijten was aan niet uitgekomen verwachtingen, zoals het niet doorgaan van een promotie of een onverwacht slechte beoordeling.

3. In de meeste gevallen droegen stressfactoren (o.a. sancties) bij aan de kansen op het misbruik door IT-medewerkers.
4. A-typische gedragingen waren vaak zichtbaar voor en na het misbruik. De medewerker gedroeg zich bijvoorbeeld opvallend vrolijk of somber.
5. De online-activiteiten van de betreffende medewerkers hadden de organisatie tijdig kunnen alarmeren of attenderen op gepland of voortgaand misbruik. Toezicht op logging van de activiteiten had misbruik kunnen voorkomen.
6. In veel gevallen negeerden organisaties de obstructie van (security-)regels, of waren zij niet in staat deze te detecteren.
7. Het afwezig zijn van voldoende fysieke en logische toegangscontrole faciliteerde het misbruik.

Veel van deze observaties zijn herkenbaar. Achteraf bleken er vaak aanwijzingen te zijn, maar een aantal daarvan is ook zeer moeilijk te plaatsen. Medewerkers met kwade bedoelingen zullen nooit te beroerd zijn om op lastige uren, wanneer alle collega's naar huis zijn, nog even door te halen om een klus af te maken. Het probleem is dat ook de meest loyale en waardevolle medewerkers dit kenmerk vertonen.

5.1.5 Classificatie van middelen

Ongewenste verspreiding

Met classificatie wordt bedoeld op het in klassen indelen van bedrijfsmiddelen en bedrijfsinformatie. Elke organisatie geeft eigen betekenissen aan de niveaus van de verschillende klassen. Indelingen naar serviceniveaus, naar vertrouwelijkheidsniveaus: er is van alles mogelijk. Belangrijk is dat zulke indelingen relevant zijn en betekenis hebben voor de medewerkers. Zo kan een vertrouwelijk document iets minder strenge verspreidingsbeperkingen kennen dan een geheim document.

Het uiteindelijke doel is om de informatie optimaal te beschermen tegen ongewenste verspreiding.

Indelingen kunnen worden gemaakt op grond van beveiligingsbehoeften of door prioriteit aan te duiden bij noodzakelijke wijzigingen en onderhoud. Middelen met een groot belang voor de organisatie kunnen bij wijzigingen worden voorzien van goede fallback-scenario's, voor het geval een wijziging niet goed uitpakt.

5.1.6 Internet is everywhere

Internet biedt onmiskenbaar kansen om kennis te vergaren, om de samenwerking met derden te optimaliseren, het bedrijfsportfolio te presenteren of om producten en/of diensten aan te bieden aan klanten. De uitgebreide mogelijkheden van internet doen bedrijven zelfs besluiten om de kernprocessen via dit medium te

ontsluiten voor ketenpartners, klanten, leveranciers en medewerkers. De traditionele fysieke scheiding tussen het interne bedrijfsnetwerk en het internet verdwijnt hierdoor.

Nieuw misbruik

Met het verdwijnen van de grenzen tussen de interne ICT en externe netwerken ontstaan nieuwe kansen op misbruik van bedrijfsmiddelen. Medewerkers die een verkeerde website bezoeken, kunnen een virus introduceren op het interne netwerk. Hackers die een lek constateren op de website kunnen proberen persoonsgegevens of creditcardinformatie uit databases te onttrekken, of via de aan de internetwebserver gekoppelde backend-systemen meeliften en zo het interne bedrijfsnetwerk binnendringen. Er zijn talloze vormen van misbruik bekend (en te verzinnen) die vanwege de koppeling met internet al realiteit zijn. Met de juiste ontwikkelstandaarden, inrichtingsstandaarden en controle-

programma's kunnen kwetsbaarheden worden voorkomen of tijdig gesignaleerd. De praktijk leert dat het rekening houden met risicoscenario's tijdens het ontwerp van pakketten en programmatuur nog in de kinderschoenen staat. In hoofdstuk 7 komen we daarop terug.

5.1.7 Falende systemen

Elke ICT-afdeling heeft wel eens meegeemaakt dat een server het onverwacht begeeft. De wet van Murphy speelt vaak een rol in de timing van zo'n incident. Goede afspraken met de leverancier over het vervangen van de hardware zijn dan onontbeerlijk om de dienstverlening weer snel te herstellen. Hetzelfde geldt voor een goede backup- en restore-oplossing, die ervoor zorgt dat de juiste data binnen de maximale uitvalsduur weer op de juiste plek beschikbaar zijn.

ELKE ICT-AFDELING HEEFT WEL EENS MEE-
GEMAAKT DAT EEN SERVER HET ONVERWACHT
BEGEEFT. DE WET VAN MURPHY SPEELT VAAK
EEN ROL IN DE TIMING VAN ZO'N INCIDENT.

5.1.8 Ontwikkelfouten en gevaarlijke achterdeurtjes

Gegevens worden benaderd met applicatie-programma's. Meestal zijn dat standaard-oplossingen, soms wordt maatwerk ingezet. Die programmatuur bevat vaak functies die niet besteld waren en niet nodig zijn. Zulke potentieel onveilige software, met (on)bewuste achterdeurtjes, verborgen functies, onjuiste functiescheidingen of programmeerfouten, kan ongewenste indringers toegang verschaffen tot het onderliggende operating-systeem. Soms zijn het ontwikkelfouten, soms is het een gewenste functionaliteit die het bedrijf zelf niet gebruikt of nodig heeft, maar waar anderen wel gebruik van willen maken.

Resistentie verzekerd?

Bij maatwerksoftware heeft de opdrachtgever de bouw van de toepassing zelf in de hand. In de ontwerpfase moeten security-eisen worden geformuleerd op basis van een zorgvuldige afweging van

de bedrijfsrisico's. In de periode van ontwikkeling tot oplevering moet de implementatie ervan structureel worden getoetst. Dat geeft zekerheid over de resistentie tegen security-inbreuken. Standaardsoftware biedt wat dat betreft veel minder zekerheid. En wat te denken van hard- en software die speciaal ontwikkeld is, zoals firewalls, encryption-software, security tokens en smartcards? Als deze producten niet correct functioneren is het bedrijfsrisico vele malen groter: de organisatie vertrouwt immers juist op deze componenten voor de beveiliging. In het dagelijks leven is dat te vergelijken met functionarissen van specialistische beveiligingsfirma's die foutief handelen door verkeerde instructies, die niet voldoen aan het vereiste profiel of, in het slechtste geval, gevoelig zijn voor corruptie en de verkeerde zaak dienen.

Veilige productie

Er zijn methodieken en best practices die ondernemingen helpen om dat risico beheersbaar te maken. Een voorbeeld daarvan zijn de zogenaamde Common Criteria (CC). Deze bieden ontwikkelaars van soft- en hardware ontwikkelaars handvatten om een veilig product te bouwen en dit te laten toetsen en certificeren. Dat geeft klanten de gelegenheid om te zien dat er serieuze aandacht is besteed aan security in de ontwikkeling van zo'n product. Bovendien krijgt de klant inzicht in de criteria die aan de ontwikkeling van het product ten grondslag hebben gelegen. Het doorlopen van een Common-Criteriacertificeringstraject is echter kostbaar. Daarom beperkt het toepassen ervan zich tot producten met voldoende product volume of producenten van securityproducten.

Het System Security Engineering-Capability Maturity Model (SSE-CMM) is ook aan een opmars begonnen. Hierbij wordt, in tegenstelling tot de Common Criteria, gekeken naar het proces waarlangs producten tot stand komen. Bij de CC staan de implementatie en toetsing van maatregelen centraal; SSE-CMM kijkt naar aspecten als: zijn de risico's inzichtelijk gemaakt bij het ontwerp? Wordt er structureel getoetst op kwetsbaarheden? Is een incident-managementproces aanwezig en hoe wordt op incidenten gereageerd? Een onderneming kan deze

methode ook gebruiken in RFI-/RFP-trajecten. De producent moet dan aantoonbaar maken hoe security is afgedekt in zijn engineeringproces.

5.1.9 Altijd beschikbaar

Op het moment dat informatie wordt toevertrouwd aan een informatiesysteem, moet erop kunnen worden gerekend dat deze informatie alleen toegankelijk is voor geautoriseerde personen. Toegankelijk is, maar ook toegankelijk blijft. De invloed die een calamiteit of (security-)incident heeft op de beschikbaarheid van informatie dient tot een acceptabele omvang te worden beperkt. Daarvoor bestaan allerlei maatregelen, zoals:

- een goede backup- en restorevoorziening waarmee informatie kan worden veiliggesteld en teruggehaald. Hieronder valt ook het periodiek testen van de voorziening;
- het verwijderen van overbodige functionaliteit uit het operating-systeem en de applicaties, waardoor deze niet kan worden ingezet om ongeautoriseerd informatie te verwijderen;
- het configureren van gedetailleerde logging- en monitoringvoorzieningen, waarmee tijdig afwijkingen binnen informatiesystemen kunnen worden gedetecteerd en de toegang tot en mutatie van informatie kan worden bewaakt.

5.1.10 Managementcyclus

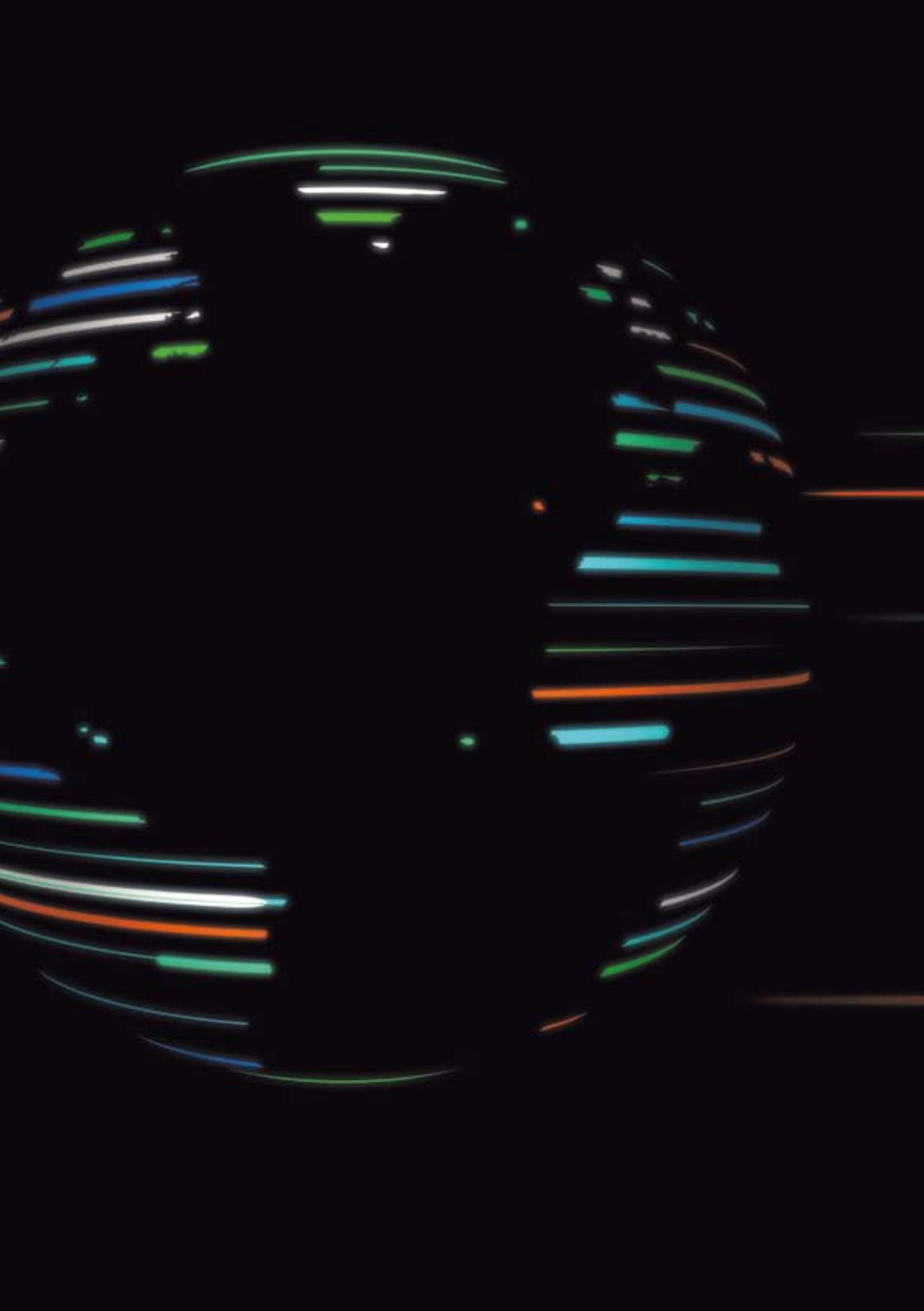
ICT-technieken bepalen doorgaans ons volledige productieproces. Er zijn veel bedrijven die hun organisatie hebben aangepast aan de mogelijkheden van bijvoorbeeld hun ERM-software. Dat is geen vreemde ontwikkeling, gezien de heersende opvatting dat standaardisatie een effectieve manier van kostenbesparing is. Dit maakt ons echter wel afhankelijk van die middelen. Zozeer zelfs, dat we in veel gevallen zijn gaan spreken van mensen die middelen ondersteunen, in plaats van andersom.

Afhankelijkheid onder controle

Om bewust te kunnen omgaan met mensen en middelen is het essentieel om een overzicht te hebben van de onderdelen waarvan we het meest afhankelijk zijn. Kunnen we die benoemen dan hebben we het overzicht over al onze afhankelijkheden en daarmee ook over de bijbehorende risico's.

Als we de risico's kennen, kunnen we maatregelen nemen. Als we maatregelen hebben genomen kunnen we ze monitoren en controleren. Als we kunnen monitoren en controleren kunnen we rapporteren. Als we kunnen rapporteren kunnen we acteren. En daarmee is de managementcyclus rond, zodat we kunnen zien of we de afhankelijkheden onder controle hebben.





6

IN HOEVERRE 'IN CONTROL'?

BUSINESS CONTINUITY MANAGEMENT, CORPORATE GOVERNANCE, COMPLIANCE, SECURITY (INFORMATIEBEVEILIGING) EN RISK MANAGEMENT ZIJN STERK GERELATEERDE DISCIPLINES DIE DE AFGELOPEN JAREN HERNIEUWD IN DE BELANGSTELLING STAAN. BEDRIJVEN HEBBEN IN TOENEMENDE MATE BEHOEFTE AAN OBJECTIEVE VERKLARINGEN OVER DE MATE WAARIN LEVERANCIERS EN/OF PARTNERS OP UITEENLOPENDE GEBIEDEN 'IN CONTROL' ZIJN. DAT HANGT SAMEN MET DE STERKE AFHANKELIJKHEID VAN BEDRIJVEN ONDERLING EN DE VAAK VERREGAANDE INTEGRATIE VAN BEDRIJFSPROCESSEN. OOK ERVAREN ORGANISATIES DRUK VAN BUITENAF. DOOR WETGEVING BIJVOORBEELD, MAAR OOK DOOR REGELGEVING DIE BRANCHES ZICHZELF OPLEGGEN OM CONTINUÏTEIT VAN ORGANISATIES TE WAARBORGEN.

Oude en nieuwe wetten

De voorbeelden zijn legio. 'Als vanouds' hebben we te maken met de Wet Bescherming Persoonsgegevens, de Wet Computercriminaliteit, de Telecomwetgeving en de Wet Elektronische Handtekening. Recenter zijn de uit de Verenigde Staten overgekomen Sarbanes Oxley Act, internationale afspraken als de Basel II en de Nationale Code Tabaksblatt. De Nederlandsche Bank, de Europese Centrale Bank en de Toezichthouder Financiële Markten hebben daarnaast hun eigen regelgeving voor de financiële wereld. De Pensioen- en Verzekeringskamer heeft dat voor de verzekeringswereld en ook de overheid heeft regelgeving voor de eigen afdelingen.

6.1 WAT DE WET DOET

DE VERSCHILLENDE WETTEN EN REGELS HEBBEN
GROSSO MODO GEMEEN DAT ZE:

- de betrouwbaarheid van het functioneren willen waarborgen;
- de verantwoordelijkheid voor dat betrouwbaar functioneren bij het bedrijfsmanagement leggen;
- daarbij uitgaan van het aantoonbaar maken van die betrouwbaarheid;
- daarvoor een aantal mechanismen aandragen, waarbij een vorm van risicoanalyse en gerelateerde maatregelen vrijwel altijd aan de orde is;
- uitgaan van een stelsel van interne en externe controle;
- in- en externe rapportage van bevindingen verlangen;
- willen zien dat het geheel functioneert en uitmondt in een aantoonbaar werkende managementcyclus.

6.2 RISICOMANAGEMENT

Het is belangrijk dat vanuit het perspectief van risicomanagement wordt gekeken naar de bedrijfsvoering, met andere woorden, dat er zicht is op de belangrijkste risico's voor een onderneming en op de houding van het bedrijf ten opzichte van deze risico's. Welke wet- en regelgeving ook van toepassing is, deze aanbeveling geldt altijd. Het bedrijf neemt, kortom, afgewogen maatregelen in de preventieve én reactieve sfeer, gericht op de continuïteit van het bedrijf én op alle relevante wet- en regelgeving.

Niet vanuit de ICT

Vooraf de volledige afhankelijkheid van ICT, maar ook ketenafhankelijkheid in het zakendoen en onzekerheden in markten, maakt de wens om 'in control' te zijn groter. De effecten van een verstoring in de ICT-diensten van een bedrijf kunnen grote impact hebben op het bedrijfsimago. Om risico's voor de bedrijfsvoering te weerstaan, moet dus niet alleen worden gekeken naar de ICT-componenten van een bedrijf, maar naar de gehele bedrijfsvoering. ICT is slechts een onderdeel. Continuïteits- en beveiligingsinitiatieven dienen daarom ook vanuit 'de business' geïnitieerd en geleid te worden en niet vanuit de ICT. Te vaak komt dat nog wél voor.

Een integrale benadering door middel van risico-inventarisatie geeft een afgewogen oordeel over de belangrijkste issues. Business Impact Analyses (BIA's) brengen in kaart welke risico's bedrijfsprocessen lopen en wat er gebeurt als deze risico's waarheid worden. Gewoonlijk worden via BIA's de kritische bedrijfsprocessen in kaart gebracht en afgezet tegen een worst-case-scenario.

Volwassen

Een goed ingericht risicomanagement (op strategisch, tactisch en operationeel niveau) is nodig om kosteneffectieve maatregelen te kunnen nemen en om aan te tonen dat de organisatie 'in control' is. De maatregelen die een bedrijf neemt, zijn afhankelijk van de volwassenheidsfase waarin het zich bevindt, de financiële middelen die het bedrijf ter beschikking staan en de externe druk die wordt uitgeoefend door bijvoorbeeld wetgevers, brancheregelgeving, auditors en aandeelhouders.

Risicomanagement wordt gedefinieerd door een aantal normen en standaarden. Op het gebied van informatiebeveiliging vigeert de ISO27001. Voor Business Continuity Management is de BS25999 beschikbaar. Beheerstandaarden geven handvatten aan de implementatie en handhaving van maatregelen: ITIL en Cobit zijn daar voorbeelden van. En er zijn talloze hulpmiddelen om het 'in control' zijn te ondersteunen. Elk van de hiervoor genoemde standaarden is voorzien van checklists en ondersteunende applicaties.

Risicomanagement is een vak geworden waarvoor specialisten kunnen worden opgeleid. Deze specialisten moeten het management ondersteunen in het analyseren, neerzetten en onderhouden van aantoonbaar betrouwbare bedrijfsprocessen.

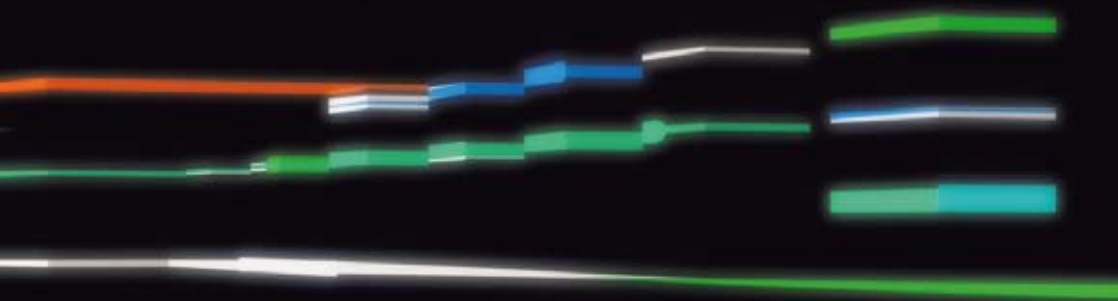
DE NOODZAAK OM 'IN CONTROL' TE ZIJN,
WORDT BEHALVE DOOR WET- EN REGELGEVING
OOK BEPAALD DOOR DE COMPLEXITEIT VAN EN
DE SNELLE VERANDERINGEN IN HET ZAKENDOEN.

6.3 WANNEER BEN IK ECHT 'IN CONTROL'?

De noodzaak om 'in control' te zijn, wordt behalve door wet- en regelgeving ook bepaald door de complexiteit van en de snelle veranderingen in het zakendoen. De behoefte aan 'dashboards' die de mate van 'in control' zijn kunnen aangeven neemt toe. Sturing op de juiste aandachtsgebieden, gebaseerd op degelijke risicoanalyses, kan hierbij helpen. Actieve ondersteuning door het gebruik van KPI's (Key Performance Indicators) helpt directies 'aan het stuur te zitten'. Om te blijven voldoen aan de eigen kwaliteitseisen en aan de eisen die wet- en regelgeving stellen, is een managementcyclus nodig waarin beleid, analyses, maatregelen, controle en terugkoppeling een volwaardige plaats hebben in het besturingsmodel, gebaseerd op eerder vastgestelde performance-indicatoren.

Klaar voor de calamiteit

Bedrijven die klaar zijn voor de toekomst en met risico's overweg kunnen, laten zien dat zij volwassen kunnen omgaan met onzekerheden. Zij hebben de vaardigheid om op een afgewogen manier risico's te hanteren, ze kunnen afdoende maatregelen nemen en hebben een goed 'dashboard' met zicht op hun belangrijkste indicatoren met betrekking tot security, corporate governance en compliance issues. En – last but not least – ook in het geval van een calamiteit zijn ze voldoende voorbereid! Zij hebben kant-en-klare maatregelen en plannen die regelmatig door de organisatie zijn geoefend en getest. ←



7 CONCLUSIE EN VISIE

7.1 ONZICHTBAARDER EN AGRESSIEVER

Het is een gegeven dat onze bedrijfsprocessen zowel van binnenuit als van buitenaf worden bedreigd. De bedreigingen zijn voor een deel bekend, maar voor een deel ook niet. Ze zijn onzichtbaarder geworden en nemen in volume en agressiviteit toe. Van oudsher hielden we daar bij het ontwerpen en inrichten van bedrijfsprocessen rekening mee. Wie is niet groot geworden met de principes van administratieve organisatie? We hielden rekening met verschillende typologieën van organisaties en hun kenmerken en pasten daar de inrichtingswijze van de organisatie op aan. Functiescheiding en

controles werden ingebouwd. Met behulp van externe- en interne controle stelden we vast of de maatregelen voldoende werden nageleefd en up-to-date waren. We noemden het niet zo, maar de hang naar 'in control' zijn is niet nieuw.

'Als het maar werkt'

Bij de intensievere automatisering en informatisering van bedrijfsprocessen hebben we misschien een aantal van bovenstaande principes uit het oog verloren. De aandacht voor functionaliteit staat voorop – het moet werken! – terwijl veiligheid en continuïteit als het ware later worden toegevoegd. Functiescheiding raakt door ingewikkelde autorisatieschema's en het onderhoud daarvan al gauw buiten beeld, of het

verwatert. Daar waar bedrijven in ketens met elkaar samenwerken, is de complexiteit groot en het geheel moeilijk te overzien. In automatiseringsland lijken drie ontwikkelingen zich asynchroon voor te doen:

- het onderhouden en uitbreiden van de functionaliteit;
- het onderhouden en uitbreiden van de beveiligingsmaatregelen;
- het onoverzichtelijker en geniepiger worden van bedreigingen.

Kortom, het lijkt een jungle te worden. Het is lastig de weg niet kwijt te raken. Maar wat we zeker niet willen is 'out of control' raken.

7.2 INTEGRALE AANDACHT EN ARCHITECTUUR

Bedrijfsprocessen zijn voor een fors deel geautomatiseerd. De ketens waarin wordt samengewerkt met externe en interne partijen worden uitgebreider, complexer en onoverzichtelijker. We kunnen het ons niet (meer) permitteren de drie hiervoor genoemde ontwikkelingen autonoom hun gang te laten gaan. We zullen die in samenhang moeten benaderen. Daarin kan maar één ding leidend zijn: de ontwikkeling van het bedrijf en de bedrijfsprocessen.

Brandvertraging

Bij de bouw of verbouw van een gebouw (en omgeving) bedenken we eerst welke eisen we stellen aan ons nieuwe onderkomen. We raadplegen een architect die ons vragen stelt over het doel en gebruik, voordat hij met een ontwerp komt.

Dat ontwerp wordt een aantal keren bijgesteld en uiteindelijk leidt dat tot een bestek op grond waarvan aannemers aan de gang kunnen.

De vereiste mate van beveiliging van een gebouw wordt vanaf de architectuur meegenomen in het ontwerp en de uitvoering. De brandvertragende materialen en afscheidingen, evenals de brand- en toegangsvoorzieningen en allerlei detectieapparatuur worden niet later ingeschroefd, maar direct bij de architectuur – afhankelijk van de behoefte – meegenomen in de bouwwijze en gebruikte materialen.

Achteraf

Het lijkt logisch dat we ook zo naar de architectuur van onze bedrijfsprocessen annex de automatisering daarvan zouden kijken. Maar hoe vaak worden, onder het mom van 'als het eerst maar werkt', de elementaire controles en veiligheidsvoorzieningen pas achteraf (of nooit) ingebouwd?

VOORAFGAAND AAN DE INRICHTING EN BOUW VAN VEILIGHEIDSMATREGELEN IN GEAUTOMATISEERDE OMGEVINGEN MOET EEN AANTAL ZAKEN DUIDELIJK ZIJN:

- de aard van de bedrijfsprocessen;
- de wijze waarop deze moeten worden ondersteund;
- de eisen die gebruikers eraan stellen;
- de omgeving waarin dit alles zich bevindt;
- de diverse in- en externe afhankelijkheden die bestaan (waaronder de wet- en regelgeving waaraan deze processen onderhevig zijn).

De traditionele opeenstapeling van maatregelen en applicaties leidt tot onbeheersbare (lees: ondoorzichtige) bedrijfsprocessen die per definitie kwetsbaar en dus niet 'in control' zijn. Het gevolg: tweemaal opsturen van belastingaangiften (maart 2008), tunnels die zich automatisch sluiten (februari 2008), et cetera.

Kwaliteit is inherent

De kwaliteit van producten en diensten wordt mede bepaald door de kwaliteit van het productieproces zelf; die kwaliteit kan niet in de slotfase zomaar aan een product of dienst worden toegevoegd. Zoals gezegd, de kwaliteit van informatievoorziening kent een aantal begrippen: betrouwbaarheid, integriteit, beschikbaarheid, effectiviteit, efficiency en controleerbaarheid.

De eerste drie vormen samen het begrip informatiebeveiliging. Dat betekent dat informatiebeveiliging (of security) onderdeel is van kwaliteit. Kwaliteit kan niet achteraf worden toegevoegd of ingebouwd, net zomin als security. Integreren in het ontwerp, in de uitvoering en in het gebruik: dat garandeert goede beveiliging die bijdraagt aan kwalitatief goede dienstverlening. Zo beschouwd zijn security en continuïteitsmaatregelen 'business enablers'. Ontbreken ze, dan ontbreekt het ook aan kwaliteit.

7.3 VISIE

Onze visie op security en continuity hangt nauw samen met het denken in architecturen, zoals hierboven beschreven. Of het nu gaat om maatregelen van administratief-organisatorische aard, om 'secure programming', robuuste en veilige gebouwen of IT-infrastructuren: in alle gevallen geldt dat security en continuity in het ontwerp moeten worden meegenomen. Direct inbouwen is goedkoper dan later aan-, bij- en verbouwen. Wij zijn ook geen voorstander van een aparte post of begroting voor beveiligingsaangelegenheden. Als we een kwalitatief goed product willen leveren, hebben we ook geen aparte post 'kwaliteit'. Die kosten horen bij de ontwikkelingskosten van dat product.

We moeten gaan voor de kwaliteit die we wenselijk achten en die past bij de producten of diensten die we willen leveren. Uiteraard met inachtneming van de voor ons geldende wet- en regelgeving. Een goede balans tussen wat wenselijk en nodig is, levert vanzelf een goede kosten-batenverhouding op.

In de haarvaten

Wij vinden het een goede zaak dat op C-level van ondernemingen steeds vaker functies te zien zijn die een leidende rol hebben in security en/of continuity. De Business Continuity Manager (BCM), de Chief Security Officer (CSO) of de Chief Information Security Officer (CISO) zijn belast met het beleid op deze gebieden. Het is hun taak om die integrale en – in onze visie – architecturale benadering gestalte te geven, te onderhouden en te bewaken. Het is hun taak om ervoor te zorgen dat op strategisch, tactisch en operationeel niveau de security- en continuïteitsmaatregelen tot in de haarvaten van het bedrijf doordringen. Een plan-do-check-act-management-cyclus op deze drie niveaus met rapportage naar het naast-hogere niveau is van belang om besturing en controle (lees: zekerstelling) te behouden. Om de integrale benadering gestalte te geven moeten deze besturing en controle zijn ingebed in de standaard-management-cycli en -rapportages. Deze visie wordt ondersteund door de

benadering die steeds meer standaarden op dit gebied voorstaan. De twee bekendste zijn de al eerder genoemde ISO27001 ('Code voor Informatiebeveiliging') en de BS25999 (Business Continuity Management Standard). Beide standaarden gaan uit van de hiervoor beschreven management-cyclus en stellen de eisen centraal die voortkomen uit de aard van de (primaire) bedrijfsprocessen.

7.4 UITBESTEDEN?

Hele bedrijfsprocessen en hun ondersteuning worden overgelaten aan externe partijen, die het beter of goedkoper zouden kunnen uitvoeren. Het is van belang om de goede beveiligings- en continuïteitseisen te stellen aan de insourcende partij én daarover te laten rapporteren. Voor de partij waaraan wordt uitbesteed gelden uiteraard minimaal dezelfde eisen als voor de eigen organisatie. De aansturing, controle en rapportage moeten aansluiten bij de binnen het uitbestedende bedrijf geldende management-rapportage.

Voordelen

Daar waar security en continuity zijn ingebed in de normale bedrijfsprocessen en integraal onderdeel uitmaken van het ontwerp, kunnen delen van de uitvoering worden uitbesteed. Ook dat moet weer zorgvuldig en gecontroleerd (= gemanaged)

AANSTURING EN CONTROLE MOETEN ZIJN INGEREGLD – DAN WORDEN HET ECHE 'MANAGED SERVICES'.

gebeuren, maar het kan de uitbestedende partij significante voordelen opleveren, zoals besparing op kosten en management- en beheertaken.

Omdat deze externe bedrijven gespecialiseerd zijn, mag (en moet) worden verwacht dat ze state-of-the-art-kennis en toepassingen hebben. Vooral op het gebied van beveiligde infrastructuur kunnen gespecialiseerde bedrijven voordeel opleveren voor de continuïteit. Uitdrukkelijk blijft daarbij overeind dat de uitbestedende partij verantwoordelijk is én blijft voor de integrale beveiliging van de eigen bedrijfsprocessen. Deze verantwoordelijkheid moet worden vastgelegd in uitbestedingscontracten. Aansturing en controle moeten zijn ingeregeld – dan worden het echte 'managed services'.

7.5 COMPLEXE VRIJHEID

Bedrijfsgegevens mogen alleen door geautoriseerden worden gezien, gemonteerd en geïnterpreteerd. Met de komst van internet, webbased applicaties en infrastructuur in het publieke en dus schijnbaar oncontroleerbare domein (denk ook aan handheld-computers en andere draagbare media), zouden we kunnen denken dat bescherming onbegonnen werk is.

Kunnen we ons binnen ons eigen domein en binnen onze eigen grenzen nog vrijheden veroorloven, daarbuiten kan dat zeker niet, want dat is een voor ons oncontroleerbare omgeving. Alles wat we in dit oncontroleerbare domein sturen en

ontvangen moet dus een zekere intrinsieke bescherming hebben. Via data-encryptie (variërend in allerlei sterkten) is dat mogelijk. Maar ook binnen ons eigen domein moeten we kunnen rekenen op een beveiligingsregime dat aansluit bij onze interne wereld en behoeften.

Vooral data beschermen

Overigens wordt die eigen interne wereld steeds kleiner. De buitenwereld wordt groter met openbare infrastructures, SAAS-oplossingen (Software As A Service) en 'thin clients' die aangesloten zijn op datacentra waar ook ter wereld. De intrinsieke beveiliging van data wordt daarmee steeds belangrijker. Vanuit die gedachte wordt ervoor gepleit om 'de muren' waardoor data worden getransporteerd te slechten en de aandacht te richten op de bescherming van de data zelf. Het blijft van belang om de eigen omgeving te kennen en af te bakenen, te voorzien van passende beschermingsmaatregelen en afspraken te hebben met de gecontroleerde omgevingen waarmee we samenwerken. Blijft over: het beschermen van de data, zodra deze het ongecontroleerde domein binnenkomen. Met andere woorden, beveiliging zal voorlopig een complex samenspel blijven van publieke en private domeinen. Dat vraagt om een uitgebalanceerde architectuur, integrale aandacht en een grondige analyse van wat wenselijk is per bedrijf of bedrijfsproces. Specialisten, inzichten, methoden en technieken

kunnen daarvoor worden ingezet om 'in control' te komen en te blijven.

7.6 CONCLUSIE

De beveiliging en continuïteit van bedrijfsprocessen verdient de aandacht van het strategische, tactische en operationele management van een onderneming. De continuïteit van de onderneming is van te veel factoren afhankelijk geworden om het toeval een kans te geven. Bovendien zijn we erg afhankelijk geworden van (informatie-) technologische ketenpartners en (inter-) nationale wet- en regelgeving. Of we nu beursgenoteerd zijn of niet, de maatschappij verlangt verantwoording en bestuurders willen continu weten hoe de vlag erbij hangt.

De risico's waaraan onze bedrijfsvoering en onze managementdoelstellingen onderhevig zijn, willen we kennen en we willen ons er gepast tegen wapenen – tegen kosten die opwegen tegen de baten. Steeds sterker heerst het besef dat beveiliging en continuïteit onlosmakelijk verbonden zijn met de kwaliteit van onze bedrijfsvoering. Als we deze zaken als add-on beschouwen, kan het wel eens onnodig kostbaar worden. We zouden zelfs in de verleiding kunnen komen om ze weg te bezuinigen. Kwaliteit zit ingebakken in producten en diensten,

vanaf het ontwerp van de architectuur tot en met de realisatie, en zelfs daarna, gedurende de onderhoudsperiode.

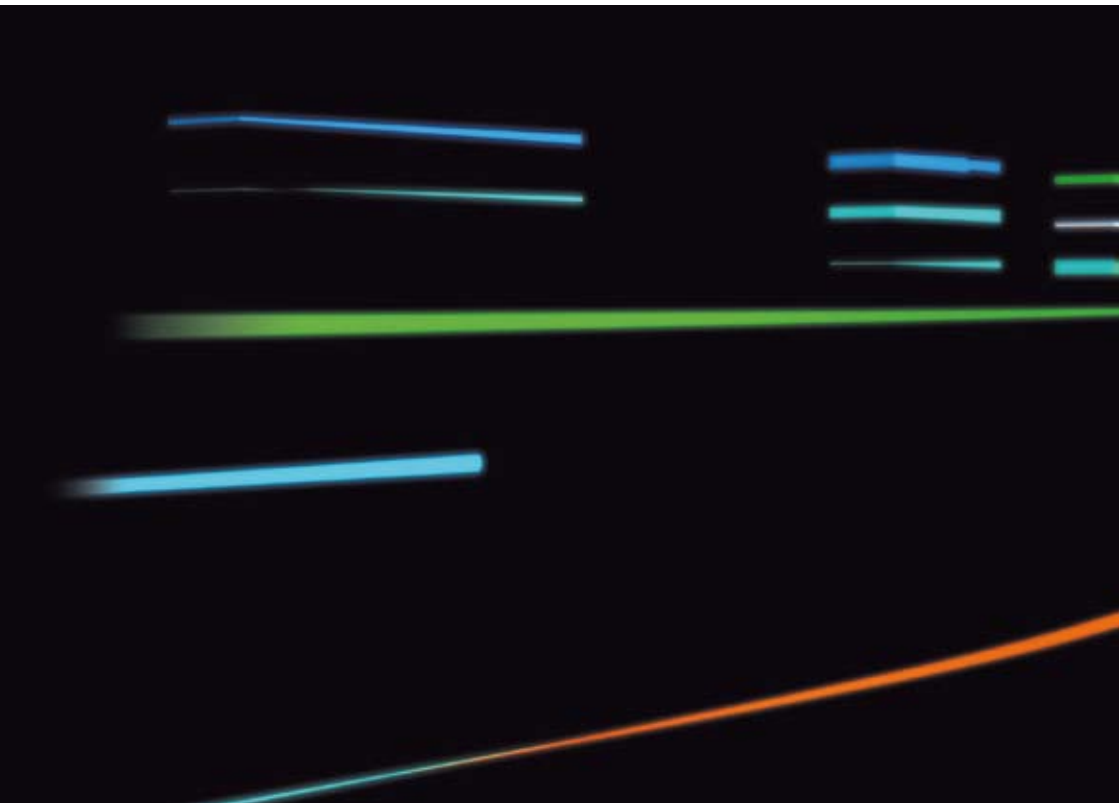
Niet later bijbouwen

Ter vergelijking kijken we naar de bouwwereld, waarin de architect van meet af aan rekening houdt met wensen van de opdrachtgever, de bouwvoorschriften kent en weet welke gebruiksdoelen worden beoogd. Het na oplevering al meteen beginnen met aan- en bijbouwen moet worden vermeden. Zo is het ook met beveiliging en continuïteit. Het direct meenemen van onze infrastructuur en applicaties in de architectuur is verreweg te verkiezen boven het later aan- en bijbouwen. Getronics heeft in dit opzicht gekozen voor de SABSA⁶-architectuur. De architect blijft bemoeienis houden, ook als eventueel later iets moet worden veranderd. De architectuur moet in stand blijven, al is het goed mogelijk om (delen van) de bouw over te laten aan gespecialiseerde externe partijen, mits iedereen werkt vanuit dezelfde architectuur en dat ook wordt gecontroleerd.

Aparte functie

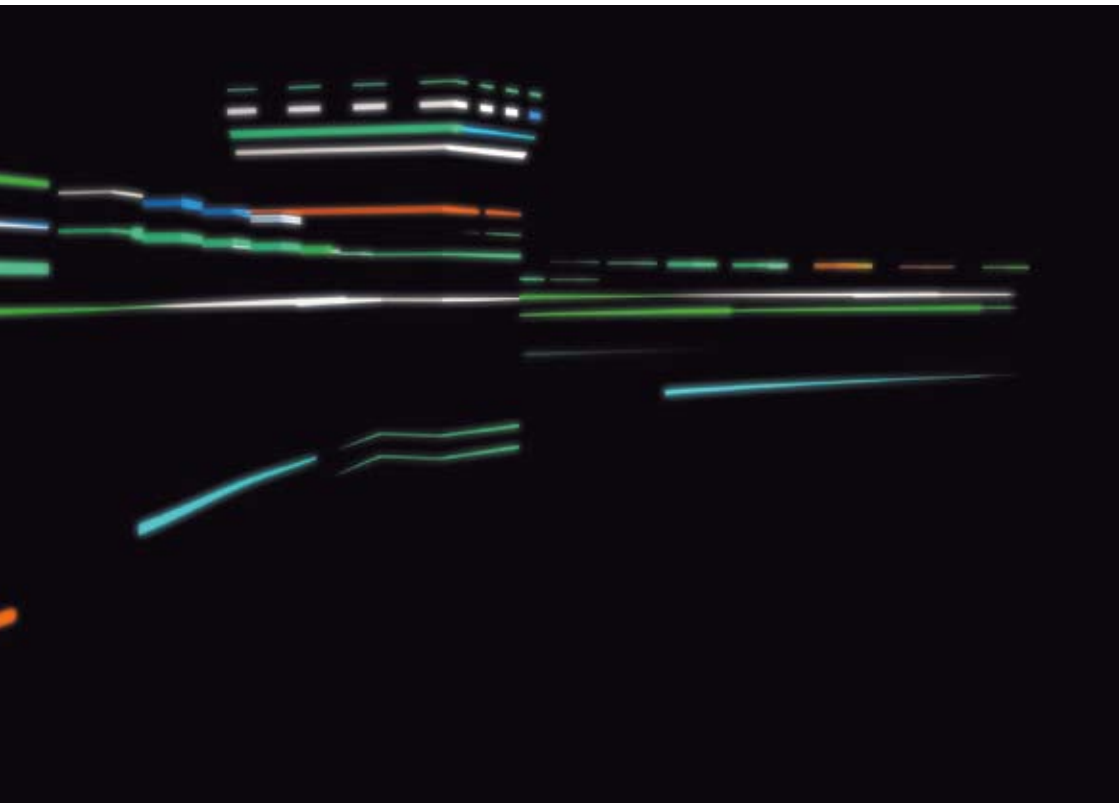
Om de kwaliteitsmaatregelen die we hebben genomen in stand te houden is constante monitoring nodig. Afhankelijk van het type en de grootte van de onderneming is een aparte functie aan te bevelen, gericht op continuïteit en beveiliging, die rapporteert aan het C-niveau. Een volwassen

6. SABSA: Sherwood Applied Business Security Architecture (a best practice method for delivering cohesive information security solutions to enterprises). (zie ook: www.sabsa-institute.org)




onderneming is voortdurend alert op veranderingen in de omgeving. Die veranderingen bieden kansen maar ook bedreigingen voor de bedrijfsvoering. De bedrijfsleiding heeft een managementcyclus nodig die monitort en rapporteert over de bestaande maatregelen; aan de andere kant moet er continu aandacht zijn voor risico's, zodat het beleid en/of de maatregelen kunnen worden bijgesteld. Uiteindelijk moet de focus van de

bedrijfsleiding niet liggen op aandacht voor continuity en security. De aandacht moet liggen op de primaire bedrijfsprocessen en de totstandkoming van producten en diensten. Als het goed is, eisen security en continuity slechts zo nu en dan de aandacht, namelijk als ze op de agenda staan en als rapportages worden besproken. In dat geval kunnen we spreken over een volwassen proces dat zichzelf in stand houdt en onderhoudt.



Bijzaak!

Als we kans zien om ons niet meer te laten verleiden tot ad-hocmaatregelen, tot incidentenpolitiek, en ons richten op een integrale benadering van security en continuïteit, gebaseerd op een gedegen architectuur, dan worden security en continuïteit bijzaak. Een bijzaak die ons helpt om onze producten en diensten met voldoende kwaliteit op de markt te brengen. ←



Deze uitgave kwam
tot stand dankzij de
medewerking van:

Albert Brouwer
Haydar Cimen
Maarten Hartsuijker
Henk Hendriks
John van Leeuwen
Huib Salomons